BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

CoRR- WO 99/35783

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2002－501218
（P2002－501218A）
(43)公表日　平成14年１月15日(2002.1.15)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　予備審査請求　有　（全 52 頁）

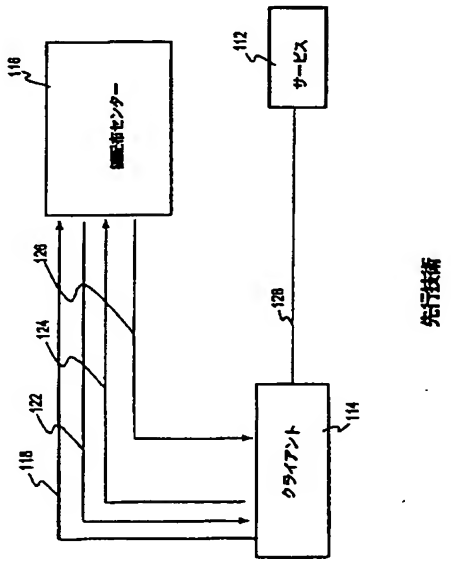
(21)出願番号　特願2000－528045(P2000－528045)
(86)（22)出願日　平成11年１月６日(1999.1.6)
(85)翻訳文提出日　平成12年７月10日(2000.7.10)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／００３４４
(87)国際公開番号　ＷＯ９９／３５７８３
(87)国際公開日　平成11年７月15日(1999.7.15)
(31)優先権主張番号　６０／０７１，０８４
(32)優先日　平成10年１月９日(1998.1.9)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／０８５，４３７
(32)優先日　平成10年５月27日(1998.5.27)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　サイバーセイフ　コーポレイション
アメリカ合衆国，ワシントン州，イサクワ，サマミツシユ　ロード，エヌ．ダブリユー．1605，スイート310
(72)発明者　ハー，マシユー
アメリカ合衆国，ワシントン州，ノースベンド，サーテイーンス　プレイス　エス．ダブリユー．1010
(72)発明者　メドビンスキー，ゲナデイ
アメリカ合衆国，ワシントン州，ベルビユー，シクス　ストリート　エス．イー．14266
(74)代理人　弁理士　東島　隆治

最終頁に続く

(54)【発明の名称】　短寿命証明書によるクライアント側公開鍵認証方法とその装置

(57)【要約】
【課題】　短寿命証明書を供給するためのシステムを効率的に実行させる能力を持つ認証システムを提供すること。
【解決手段】　鍵配布センター（ＫＤＣ）は公開-秘密鍵ペアーと証明書テンプレートを生成し格納する。ユーザーはＫＤＣ中に格納されている公開-秘密鍵ペアーを割り当てられる。ＫＤＣに対して認証を求めるユーザーは（たとえば、カーベロスシステムによるパスワードを用いて）、システムに対して短寿命証明書を生成、署名することによってユーザーの公開鍵を再証明することを促す。



先行技術

【特許請求の範囲】

【請求項１】　チケットプロトコルに従ってチケットを出力するように構成された少なくとも第１の鍵配布コンピューターにネットワークによって結合された、少なくとも第１のクライアントコンピューターを含む、前記ネットワーク内のユーザーに対して公開鍵証明書を発行するためのコンピューターを用いた方法であって、その方法は：

前記鍵配布コンピューターにアクセスできるメモリーに、少なくとも、前記ユーザーの公開鍵を格納すること、

前記クライアントコンピューター中で、少なくとも前記ユーザーの初回のパスワードを受信すること、

前記クライアントコンピューター中で前記パスワードの有効性を検証すること、

前記クライアントコンピューターから前記ネットワークを通して前記鍵配布コンピューターに、少なくとも前記ユーザーの身元確認の標識を含む初回のメッセージを発信すること、及び

初回に、前記初回のメッセージに応答して、前記鍵配布コンピューターからネットワークを通して前記クライアントコンピューターに前記チケットプロトコルによるチケットと前記ユーザーの前記公開鍵を含む短寿命の公開鍵証明書の両方を発信すること、

を具備する、公開鍵証明書を発行するためのコンピューターを用いた方法。

【請求項２】　前記チケットプロトコルがカーベロスプロトコルである請求項１で請求されたコンピューターを用いた方法。

【請求項３】　前記初回のメッセージに応答して前記鍵配布センターからネットワークを通して前記クライアントコンピューターに、前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵を発信することを、さらに含む請求項１で請求されたコンピューターを用いた方法。

【請求項４】　前記短寿命の公開鍵証明書が前記初回の後約１週間以下の有効期間を持つ請求項１で請求されたコンピューターを用いた方法。

【請求項５】　前記短寿命の公開鍵証明書が前記初回の後約１２時間以下の

有効期間を持つ請求項１で請求されたコンピューターを用いた方法。

【請求項６】　前記ユーザーの認証を提供する前記短寿命の公開鍵証明書を用いることをさらに含む請求項１で請求されたコンピューターを用いた方法。

【請求項７】　公開鍵システムによって制御される資源を前記ユーザーが使用する権限を与える前記短寿命公開鍵証明書の使用をさらに含む請求項１で請求されたコンピューターを用いた方法。

【請求項８】　前記公開鍵証明書がＸ．５０９証明書である請求項１で請求されたコンピューターを用いた方法。

【請求項９】　チケットプロトコルに従ってチケットを出力するように構成された少なくとも第１の鍵配布コンピューターにネットワークによって結合された、少なくとも第１のクライアントコンピューターを含む、前記ネットワーク内のユーザーに対して公開鍵証明書を発行するするための装置であって、その装置は、

前記鍵配布コンピューターにアクセスできる、少なくとも前記ユーザーの鍵を格納するためのメモリー、

前記クライアントコンピューター中で少なくとも前記ユーザーの初回のパスワードを受信し、前記クライアントコンピューター中で前記パスワードの有効性を検証し、前記クライアントコンピューターから前記ネットワークを通して前記鍵配布センターに、少なくとも前記ユーザーの身元確認の標識を含む初回のメッセージを発信し、

初回に、前記初回のメッセージに応答して、前記鍵配布センターからネットワークを通して前記クライアントコンピューターに前記チケットプロトコルによるチケットと前記ユーザーの前記公開鍵を含む短寿命の公開鍵証明書の両方を発信するよう、

プログラムされた前記クライアントコンピューターと前記鍵配布コンピューター、

を具備する、公開鍵証明書を発行するための装置。

【請求項１０】　前記チケットプロトコルがカーベロスプロトコルである請求項９で請求された装置。

【請求項１１】　前記初回のメッセージに応答して前記鍵配布センターからネットワークを通して前記クライアントコンピューターに、前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵をさらに発信する請求項９で請求された装置。

【請求項１２】　前記短寿命の公開鍵証明書が前記初回の後約１週間以下の有効期間を持つ請求項９で請求された装置。

【請求項１３】　前記短寿命の公開鍵証明書が前記初回の後約１２時間以下の有効期間を持つ請求項９で請求された装置。

【請求項１４】　前記ユーザーの認証を提供する前記短寿命の公開鍵証明書を用いることを、さらに具備する請求項９で請求された装置。

【請求項１５】　公開鍵システムによって制御される資源を前記ユーザーが使用する権限を与える前記短寿命公開鍵証明書の使用をさらに具備する請求項９で請求された装置。

【請求項１６】　前記公開鍵証明書がＸ．５０９証明書である請求項９で請求された装置。

【請求項１７】　前記ネットワークによって、チケットプロトコルに従ってチケットを出力するように構成された少なくとも第１の鍵配布コンピューターに結合された、少なくとも第１のクライアントコンピューターを含む前記ネットワーク内のユーザーのための公開鍵証明書を発行するするための装置であって、その装置は、

前記鍵配布コンピューターにアクセスできる、少なくとも前記ユーザー鍵を格納するためのメモリー手段、

前記クライアントコンピューターに結合し、少なくとも前記ユーザーの初回パスワードを受信するための手段、

前記クライアントコンピューター中で前記パスワードの有効性を検証するための手段、

前記クライアントコンピューターに結合し、前記クライアントコンピューターから前記ネットワークを通して前記鍵配布センターに、少なくとも前記ユーザーの身元確認の標識を含む初回のメッセージを発信するための手段、

前記鍵配布コンピューター中で、初回に、初回のメッセージに応答して、前記鍵配布コンピューターからネットワークを通して前記クライアントコンピューターに前記チケットプロトコルによるチケットと前記ユーザーの前記公開鍵を含む短寿命の公開鍵証明書の両方を生成し、発信するための手段、

を具備する、公開鍵証明書を発行するための装置。

【請求項１８】　前記初回のメッセージに応答して前記鍵配布センターからネットワークを通して前記クライアントコンピューターに、前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵を発信するための手段をさらに具備する請求項１７で請求された装置。

【請求項１９】　前記短寿命の公開鍵証明書が前記初回の後、約１週間以下の有効期間を持つ請求項１７で請求された装置。

【請求項２０】　前記短寿命の公開鍵証明書が前記初回の後、約１２時間以下の有効期間を持つ請求項１７で請求された装置。

【請求項２１】　前記ユーザーの認証を提供する前記短寿命の公開鍵証明書を用いることを、さらに具備する請求項１７で請求された装置。

【請求項２２】　公開鍵システムによって制御される資源を前記ユーザーが使用する権限を与える前記短寿命公開鍵証明書の使用をさらに具備する請求項で請求された装置。

【請求項２３】　前記公開鍵証明書がＸ．５０９証明書である請求項１７で請求された装置。

【請求項２４】　ユーザーに対して公開鍵証明書を発行するするためのコンピューターを用いた方法であって、その方法は、

前記ユーザーに関連する公開鍵を含む複数の公開鍵を、前記コンピューターに結合したメモリーに格納すること、

前記ユーザーの身元確認を含むメッセージを、複数の任意の時間に、前記コンピューターで受信すること、

少なくとも初回の複数の前記各メッセージに応答して、前記ユーザーに関連した前記公開鍵の標識と前記証明書に対する有効期間の標識を含み、同一の公開鍵の標識と異なった一連の有効期間を持つ一連の公開鍵証明書が出力される、前記

ユーザーに対する公開鍵証明書を、出力すること、

を具備する、ユーザーのための公開鍵証明書を発行するためのコンピューターを用いた方法。

【請求項２５】　前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵が前記公開鍵が出力されるときはほぼ常に出力される請求項２４で請求されたコンピューターを用いた方法。

【請求項２６】　前記シーケンス中の各公開鍵証明書は、ほぼ前記証明書が発行されてから前記証明書の失効時期までの有効期間を持っており、前記シーケンスにおける各公開鍵証明書は、約１週間よりも短い有効期間を持っていて、従って、公開鍵証明書の前記シーケンスが短寿命証明書のシーケンスとなるような請求項２４で請求されたコンピューターを用いた方法。

【請求項２７】　前記シーケンス中の前記各公開鍵証明書が約１日以下の有効期間を持つ請求項２４で請求されたコンピューターを用いた方法。

【請求項２８】　前記シーケンス中の前記各公開鍵証明書が約１２時間以下の有効期間を持つ請求項２４で請求されたコンピューターを用いた方法。

【請求項２９】　ユーザーのための公開鍵証明書を発行するための装置であって、その装置は、

前記ユーザーに関連した公開鍵を含む複数の公開鍵を格納するためのコンピューターに結合されたメモリー、

前記ユーザーの身元確認を含むメッセージを複数の任意の時間に受信する能力を持つようにプログラムされたコンピューター、

少なくとも初回の複数の前記各メッセージに応答して、前記ユーザーに関連した前記公開鍵の標識と前記証明書に対する有効期間の標識を含み、同一の公開鍵の標識と異なった有効期間のシーケンスを持つ公開鍵証明書のシーケンスが出力される前記ユーザーに対する公開鍵証明書を出力するようプログラムされた前記コンピューター、

を具備する、ユーザーのための公開鍵証明書を発行するための装置。

【請求項３０】　前記コンピューターが、前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵が前記公開鍵が出力されるときは、ほぼ常に出力され

るようプログラムされている請求項２９で請求された装置。

【請求項３１】　前記シーケンス中の各公開鍵証明書が、ほぼ前記証明書が発行されてから前記証明書の有効期間までの有効期間を持っており、前記シーケンスにおける各公開鍵証明書が約１週間よりも短い有効期間を持っていて、従って、公開鍵証明書の前記シーケンスが短寿命証明書のシーケンスであるような請求項２９で請求された装置。

【請求項３２】　前記シーケンス中の前記各公開鍵証明書が約１日以下の有効期間を持つ請求項２９で請求された装置。

【請求項３３】　前記シーケンス中の前記各公開鍵証明書が約１２時間以下の有効期間を持つ請求項２９で請求されたコンピューターを用いた方法。

【請求項３４】　ユーザーのための公開鍵証明書を発行するための装置であって、その装置は、

前記ユーザーに関連した公開鍵を含む複数の公開鍵を格納するためのコンピューターに結合されたメモリー手段、

前記ユーザーの身元確認を含むメッセージを複数の任意の時間に受信するようにプログラムされたコンピューター、

少なくとも初回の複数の前記各メッセージに応答して、前記ユーザーに関連した前記公開鍵の標識と前記証明書に対する有効期間の標識を含み、同一の公開鍵の標識と異なった有効期間のシーケンスを持つ公開鍵証明書のシーケンスが出力される前記ユーザーに対する公開鍵証明書を出力するようプログラムされた前記コンピューター、

を具備する、公開鍵証明書を発行するための装置。

【請求項３５】　前記公開鍵が出力されるときは、前記ユーザーの前記公開鍵に対応する前記ユーザーの秘密鍵をほぼ常に出力するための手段をさらに具備する請求項３４で請求された装置。

【請求項３６】　前記シーケンス中の各公開鍵証明書が、ほぼ前記証明書が発行されてから前記証明書の失効時期までの有効期間を持っており、前記シーケンスにおける各公開鍵証明書が約１週間よりも短い有効期間を持っていて、従って、公開鍵証明書の前記シーケンスが短寿命証明書のシーケンスであるような請

求項３４で請求された装置。

【請求項３７】　前記シーケンス中の前記公開鍵証明書が約１日よりも短い有効期間を持っている請求項３６で請求されたコンピューターを用いた方法。

【請求項３８】　前記シーケンス中の前記公開鍵証明書が約１２時間よりも短い有効期間を持っている請求項３６で請求されたコンピューターを用いた方法。

【請求項３９】　ユーザーに対する公開鍵証明書を発行するためのコンピューターを用いた方法であって、その方法が、

前記コンピューター中で前記ユーザーの身元確認を含むメッセージを受信し、

前記受信ステップに応じて、短寿命公開鍵証明書を出力する、

ことを具備する方法。

【請求項４０】　ユーザーに対する公開鍵証明書を発行するための装置であって、その装置は、

前記ユーザーの身元確認を含むメッセージを受信し、前記メッセージに応じて短寿命公開鍵証明書を出力するようにプログラムされたコンピューターを具備する装置。

【請求項４１】　ユーザーに対する公開鍵証明書を発行するための装置であって、その装置は、

前記ユーザーの身元確認を含むメッセージを受信するためのコンピューターを用いた手段、

ユーザーに対する公開鍵証明書を発行するための装置であって、その装置は、

前記メッセージの受信に応じて短寿命公開鍵証明書を出力するするためのコンピューターを用いた手段、

を具備する装置。

【請求項４２】　最初のスマートカードプロトコルに従ってユーザーを認証するよう構成したコンピューターを用いた認証システムであって、資源に対する認証のための方法が、

最初のユーザーの公開－秘密鍵ペアーを供給すること、及び、

前記鍵ペアーを用いて、前記スマートカードプロトコルに従ってスマートカー

ドが生成するレスポンスを模擬すること、

を具備する方法。

【請求項４３】　前記公開-秘密鍵ペアー公開鍵が前記ユーザーの短寿命公開鍵証明書によって証明される請求項４２で請求された方法。

【請求項４４】　コンピューターを用いた公開鍵証明法であって、その方法は、

公開鍵と秘密鍵のペアーを取得し、

前記公開鍵に対する一連の公開鍵証明書を、年当たり少なくとも２通の公開鍵証明書生成の頻度で生成する、

ことを具備する方法。

【請求項４５】　前記頻度が年当たり少なくとも約１２通の公開鍵証明書である請求項４４で請求された方法。

【請求項４６】　前記頻度が週当たり少なくとも約５通の公開鍵証明書である請求項４４で請求された方法。

【請求項４７】　前記公開鍵証明書が約６ヶ月以下の証明書寿命を決める有効期間を具備する請求項４４で請求された方法。

【請求項４８】　前記公開鍵証明書が約１週間以下の証明書寿命を決める有効期間を具備する請求項４４で請求された方法。

【請求項４９】　前記公開鍵-秘密鍵ペアーが少なくとも約１年の公開鍵-秘密鍵ペアー寿命を決める有効期間を持つ請求項４４で請求された方法。

【請求項５０】　前記公開鍵-秘密鍵ペアーが約１年以下の公開鍵-秘密鍵ペアー寿命を決める有効期間を持つ請求項４４で請求された方法。

れた方法。

【請求項５１】　前記公開鍵証明書が約１日以下の証明書寿命を決める有効期間を具備する請求項５０で請求された方法。

【請求項５２】　通信リンクによって結合された少なくとも１台のクライアントコンピューターと少なくとも１台のサーバーコンピューターを持つコンピューターシステムにおいて用いるための方法であって、その方法は、

前記コンピューターシステムに結合されたメモリー中に、通常スマートカード

上にしまわれたタイプの少なくともある量のデータを表す初回の情報を格納すること、

ユーザーのパスワードベースの認証に対するカーベロス型システムを用いること、及び、

前記パスワードベースの認証に続いて前記最初の情報を取り出すこと、

を具備する方法。

【請求項５３】　前記初回の情報を用いてハードウエアスマートカードの使用を模擬することををさらに具備する請求項５２で請求された方法。

【請求項５４】　前記初回の情報が、対称鍵、非対称鍵ペアーおよび鍵証明書の少なくとも１つを具備する請求項５２で請求された方法。

【請求項５５】　前記公開鍵証明書がさらに権限付与情報を含んでいる請求項４４で請求された方法。

【請求項５６】　前記権限付与情報がグループ帰属情報を具備する請求項５５で請求された方法。

【請求項５７】　前記権限付与情報を資源権限付与システムにおいて用いることをさらに具備する請求項５５で請求された方法。

【請求項５８】　ユーザー認証のための装置であって、その装置は、

ハードウエアスマートカードを受信し、受信した前記ハードウエアスマートカードを用いてユーザーを認証する手段、および、

ハードウエアスマートカードを受信し、受信した前記ハードウエアスマートカードを用いてユーザーを認証する手段、

を具備する装置。

【請求項５９】　物理的なスマートカードにログインすることを模擬するためのコンピューターを用いた方法であって、その方法は、

クライアントコンピューターを用いて、クライアントアプリケーションログインリクエストにこたえてユーザーからのパスワード入力を促すこと、

前記パスワードの前記サーバーコンピューターへの送出がない場合には、少なくとも、ユーザーを身元確認するリクエストを持っている最初のサーバーコンピューターにメッセージを送ること、

前記サーバーコンピューターから前記クライアントコンピューターに、少なくとも部分的に暗号化してスマートカードイメージを送ること、及び、

前記スマートカードイメージからの少なくとも一部を用いて前記クライアントコンピューターにメッセージを送ることによって、、物理的スマートカードからの応答を模擬すること、

を具備する方法。

【請求項６０】　前記スマートカードイメージが公開鍵証明書を含む請求項５９で請求された方法であって、その方法は、

前記公開鍵証明書が失効しているか否かを判断すること、

前記の公開鍵証明書が失効している場合には、サーバーコンピューターに対して証明書の請求を送ること、

を具備する方法。

【請求項６１】　前記スマートカードイメージを更新するために、前記クライアントコンピューターからの情報を前記第１のサーバーコンピューターに送ることをさらに具備する請求項５９で請求された方法.

【請求項６２】　物理的なスマートカードにログインすることを模擬するための装置であって、その装置は、クライアントコンピューターを用いて、クライアントアプリケーションログイン請求にこたえてユーザーからのパスワード入力を促す手段、

クライアントコンピューターを用いて、クライアントアプリケーションログイン請求にこたえてユーザーからのパスワード入力を促す手段、

前記パスワードの前記サーバーコンピューターへの送出がない場合には、少なくとも、ユーザーを身元確認するリクエストを持っている最初のサーバーコンピューターにメッセージを送るための手段、

前記サーバーコンピューターから前記クライアントコンピューターに、少なくとも部分的に暗号化してスマートカードイメージを送る手段、また、

前記スマートカードイメージからの少なくとも一部を用いて前記クライアントコンピューターにメッセージを送ることによって、物理的スマートカードからの応答を模擬する手段、

を具備する装置。

【請求項６３】　ネットワークによって、少なくとも第１のサーバーコンピューターに結合された第１のクライアントコンピューターを含むそのネットワーク中の物理的なスマートカードにログインすることを模擬するための装置であって、それは、

少なくとも第１のスマートカードイメージを表す情報を格納するための、前記サーバーコンピューターにアクセスできるメモリーを具備し、

前記のクライアントコンピューター及びサーバーコンピューターは：

前記クライアントコンピューターを用いて、クライアントアプリケーションログイン請求にこたえてユーザーからのパスワード入力を促し、

前記パスワードの前記サーバーコンピューターへの送出がない場合には、ユーザーを身元確認するリクエストを具えた少なくとも前記第１のサーバーコンピューターにメッセージを送り、

前記サーバーコンピューターから前記クライアントコンピューターに、

少なくとも部分的に暗号化したスマートカードイメージを送り、且つ、

前記スマートカードイメージからの情報の少なくとも一部を用いて前記クライアントコンピューターにメッセージを送り、それによって、物理的スマートカードからの応答を模擬する、

ようにプログラムされている、

ものである装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は公開鍵認証（オーセンティケーション）システム、特にクライアント側公開鍵の認証の実行を可能とするシステムに関する。

【０００２】

【発明が解決しようとする課題】

初期の情報セキュリティーシステムの１つは、秘密確保のための暗号の開発、ならびに暗号化と復号化が主な問題であった。最近特に、エレクトロニクス通信とコンピューターベースの情報システムでは、情報セキュリティーシステムが認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）（メッセージが真に表記されている発信元からのものかどうかを確認する）とか権限付与（Ａｕｔｈｏｒｉｚａｔｉｏｎ）（ハードウエア、ソフトウエア、またはデータへの認可のない使用者のアクセスの防止）など、秘密確保以外の目的にも使われるようになってきている。

【０００３】

本発明は、情報セキュリティーの多くの分野に適用できるであろうし、また、多くの分野に関連しているが、その最も直接的な応用は、クライアント側の公開鍵の認証についてである。典型的には、認証が生起した後、認証がアクセス制御の決定を行うなど、認証はその後の決定についての基礎を形成するものである。

【０００４】

多くのセキュリティーシステムは基本的には、データの暗号化システムに関係している。データを暗号化し、また復号化するシステムが発展してきて、多くの工夫がこらされた方式が出てきたが、情報のプライバシーと暗号化の間には密接な関係があることは明らかである。暗号化は、種々のやりかたで身元確認と認証に関係を持たせることができる。

【０００５】

暗号化されたメッセージの受信者が、暗号化に使われた鍵を持っているのは一人の人だけだということを確信できるなら、復号化が無事行われたということだけで身元確認とまたある程度の認証を達成したことになる、という場合が、最も

明瞭な場合である。認証の目的のために暗号化を使えば、資源（リソース）の管理を、アクセス要求者の認証によって行うことができるので、アクセス制御に役立つことは明らかである。

【０００６】

パスワードにもとづく認証システムでは、パスワードの権限のない者への漏洩を防ぐのに、（パスワードを送信したり格納したりする前に暗号化したり、対称鍵に変換したり、また、ユーザー認証用の暗号化ベースのプロトコルに使うなどして）暗号化を使うことができる。

【０００７】

暗号化システムは、それ以外のシステムもあるが、しばしば秘密鍵（「対称鍵」）のシステムと公開鍵（「非対称鍵」）のシステム（時としてこれらは、公開鍵プライベート鍵のシステムとも呼ばれる）に分類される。典型的な秘密鍵システムまたは対称鍵システムでは、暗号化と復号化の両方に同じ鍵が使われる。このシステムでは、たとえば、権限を持つ人（複数）だけが鍵の内容を知っているか、あるいは秘密鍵を分け持つか、などして鍵の秘密を保つことが重要である。

【０００８】

したがって、この秘密鍵システムの１つの困難な点は、秘密を保持することである。もうひとつの困難な点は鍵の複製である。もし当事者が２人あるいは２人以上の人と通信を希望するが、その通信に全ての関係者をアクセスさせることを必ずしも希望しない場合、一般的には、各１対の当事者間ごとに1種類の鍵を共有することが必要になる。このような鍵を管理し配布することは、大きな組織ではかさばってしまって扱いにくいものとなる。

【０００９】

それについての１つの解決法は信頼できる第三者機関（ＴＴＰ（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ））を設立することである。ＴＴＰを設立すれば、各当事者は当事者とＴＴＰとの間の鍵を１個持つだけでよく、ＴＴＰがどのような個別の通信のチャンネルの確立に対しても仲介の役を果たしてくれるものである。このシステムは、多くの目的に有用であるが、ＴＴＰ自体のセキュリティーを如何にして確保するかということとホストの鍵の秘密を保持する点に困難性が

ある。

【００１０】

ある程度の成功を収めたＴＴＰ の実施例として、一般的にカーベロスとして知られている以下に詳しく述べるものがある。ここで用いている「カーベロス型のシステム （kerberos like system）」という語は一般に、カーベロス、すなわち、ユーザーとサービスとの間で対称鍵を分け持たせる信頼できる第三者機関のことを指している。カーベロス型システムは多くの状況下で非常に有用であることがわかっているが、従来のカーベロス型システムは、典型的には、公開鍵システムに伴う利点（たとえばディジタル署名のような）を提供するようにはつくられていないと考えられている。

【００１１】

公開鍵（ＰＫ，Ｐｕｂｌｉｃ Ｋｅｙ）システムでは、情報を保護するために２個の相対応する鍵（非対称鍵）が使われる。２個の鍵のうちの１個の鍵で暗号化された情報はもう１つの鍵でしか復号化することができない。ある公開鍵システムでは、２個の鍵の何れかが暗号化に使われ、もう１つの鍵が復号化に使われる。また他のシステムでは、１個の鍵が暗号化にだけ使われ、もう１つの鍵は復号化にだけ使われる。

【００１２】

公開鍵システムの１つの重要な特徴は、２個の鍵のうちの１個の鍵の知識を使ってもう１つの鍵の内容を計算によって知ることはできないということである。典型的には公開鍵システムでは、システムの各ユーザーは１（ひと）組の２個のこのような鍵を持っている。１つの鍵は秘密を保っており、もう１つの鍵は自由に公開されている。もし送信者が受信者の公開鍵でメッセージを暗号化したならば、送信者によって意図された受信者だけがそのメッセージを復号化できる（なぜなら、その受信者だけが、公表された公開鍵に対応する秘密鍵を所持しているからである）。

【００１３】

もし送信者が上の暗号化の実行に先立ってメッセージの初回の暗号化を送信者の秘密鍵を用いて実行し、（受信者の秘密鍵を用いて）受信者は初回の復号化を

行い、さらにその結果を（送信者の公開鍵を用いて）復号化したならば、秘匿性のみならず認証も保証されたことになる；何故ならば、送信者だけが、送信者の公開鍵で成功裡に複号化できるようなメッセージを暗号化できるからである。

【００１４】

ある１つのディジタル署名方式では、１方向ハッシュ関数がまずメッセージに適用され、メッセージのハッシュが送信者の秘密鍵によって暗号化される。

このシナリオでは、受信者がメッセージの発信元について持つ信頼の程度は、送信者の公開鍵が送信者だけによって保持されている秘密鍵に対応しているはずだということ対する受信者の信頼の程度に依存している。多くの現行のシステムにおいては、一般に、この種の信頼度を提供するために、多くの信頼度の高い証明機関が設立されてきた。

【００１５】

現在最も広く使われているシステムでは、それらの機関が公開鍵の証明書を発行している。最も広く使われている証明書の標準（国際標準機構（ＩＳＯ，International Standard Organization）と国際電信電話諮問委員会（ＣＣＩＴＴ，Comite Consuktatif Internationale Telegraphique et Telephonique によって決められた標準 Ｘ.５０９）のもとでは、証明書は公開鍵、公開鍵の所持者の名前あるいは公開鍵に関係する者の名前、その他、例えば有効期間などの情報を含んでおり、それらが信頼できる関係者によってディジタル的（したがって、暗号化または他の変形された形で）に署名されている。

【００１６】

ディジタル署名は、たとえば、ディジタル署名標準（ＤＳＳ（Digital Signature Standard））（エヌアイエスディ（National Institute of Standard and Technology）国家標準技術局）にもとづいて発行される。典型的には、ディジタル署名は１方向ハッシュをかけた後、さらに証明機関の秘密鍵で暗号化するステップを含んでいる。このようなディジタル署名は、信頼できる機関の秘密鍵を用いて発行され、それはまた、信頼できる関係機関によって署名されたいま１つの信頼できる関係機関の証明書を用いて認証されというように、信頼できる機関の多重の階層による証明によって認証されている。

【００１７】

公開鍵システムは、インターネット上のブラウジングを含む多くの状況下で使われているが、その経験によれば、公開鍵システムは、それ自身多くの問題点を持っていることがわかってきた。ある程度受け入れ可能な程度のセキュリティーを提供しようとすると、ユーザーが秘密を保持している鍵を記憶することはできなくなる（典型的には、１０２４ビットの２進数のような大きな数である）。そこで、実際には、それをどこかにしまわなければならず、そうすると、それは壊れやすいものであり、セキュリティーに対しても防備が薄くり、また、多くのシステムでは、特殊なハードウエアを必要とすることになる（たとえば、スマートカードとか、場合によっては、特別のコンピューターが必要となる）。

【００１８】

従来システムの１つでは、スマートカードが認証システムの一部をなしている。多くのスマートカードシステムと用法は既知である。たとえば、セキュア・ソケット・レイヤー（ＳＳＬ:Secure Socket Layer）プロトコルはクライアントに適用する際、あるサービスとの通信を確立するのにディジタル署名を要求する。ある種の環境下では、スマートカードがこのようなディジタル署名に使われる情報を持っており、それによってユーザーは、これに適するスマートカードを持っておれば（例えば、鍵を覚えていなくても）、このような資源にアクセスすることができる。公開鍵と秘密鍵の対を使うところの、これ以外のスマートカード認証の手順も既知である。

【００１９】

現在用いられているプリンシプル・スマートカード・インターフェースはＰＫＣ＃１１（公開鍵暗号標準、ＲＳＡデータセキュリティー・インク）とＰＣ/ＳＣ（パーソナルコンピューター/スマートカード）である。

【００２０】

上に述べたような証明書は典型的には、有効期間つきで提供されている。このような有効期間は、現在のシステムでは、通常、発行から１年または１年以上の単位で、比較的その寿命が長い。公開鍵システムが魅力的であると考えられている特徴の１つはその使用が容易なことであるから、もしユーザーが頻繁に鍵のペ

アーを受け取って、新しい公開鍵をその都度公示しなけらばならないとすれば、このような特徴は大いに損なわれることになる。しかし、場合によっては、以前に発行された証明書を取り消すことが必要となる。

【００２１】

たとえば、会社の高度な情報への従業員のアクセスを制御するのに使われる一対の公開鍵は、その従業員がその会社を退職したとき取り消されなければならない。したがって、従来の公開鍵システムの信頼度は、普通、証明書取り消しリスト（ＣＲＬ，Certificate Revocation List）に対して証明書をチェックすることに頼っていることになる。Ｘ．５０９標準はＣＲＬ表示の１つの例を示している。しかし、不幸なことには、このことは、例えば、イントラネットあるいはインターネットの広がりの配布を必要とし、さらに付加的なチェックまたは比較のステップを必要とする。これらは、比較的大きな企業とかネットワークでは大きな負担となり、システムが維持できなくなる。

【００２２】

公開鍵システムに伴うもうひとつの難点は秘密鍵の配布と管理である。例えば、ある会社が新しく従業員（複数）を雇用したとする。そのある従業員（複数）には公開鍵-秘密鍵のペアーを配布しようとするが、このようなやり方で秘密鍵を配布することは、秘密鍵が部外者に漏らされることを防止する上で問題がある。秘密鍵が目的通りに使われていれば従業員の秘密鍵の秘密は守られるだろうが、それらの秘密鍵に会社が直接アクセスすることを必要とするかも知れない状況（たとえば、現在退職してしまっている従業員によって過去に暗号化された会社所有の情報を得ようとする場合のように、）が起こることがある。

【００２３】

しかし、従業員の鍵を、例えば、未交付捺印証書（エスクロウ；従業員の鍵を予め第三者に託しておき、従業員が退職したときに鍵の引渡しを受けるもの）として保管するのも、典型的には、大きな管理努力と費用を伴うだろう。

【００２４】

したがって、公開鍵の技術が使えて、たとえば、ＣＲＬチェックシステムの荷重（負担）を軽減または除去しながら、セキュリティーに関して妥協を許さずに

（たとえば、従来のシステム下で証明書を取り消されるところの退職者などのリストを作成するなどして）、同時にコンピューターネットワークのセキュリティーが維持できるシステムが提供できるならば、その価値は非常に大きい。

【００２５】

また、秘密鍵の配布と管理に伴う努力と出費を軽減または除去できるシステムを提供することも有用である。また、従来のシステムに付随していたハードウエア依存性、および/または、セキュリティー・リスクを軽減または除去しつつ、秘密鍵保管の目標が達成できるような公開鍵システムを提供することも有用である。

【００２６】

それに加えて、現用のシステムの持つ特徴の利点を生かして、そのような特徴を実行するための現行システムに対する開発、プログラミングおよび変更の総量を最小にしながら、そのような改良された公開鍵システムを提供することは有用なことである。

【００２７】

【発明の概要、課題を解決する手段、発明の効果】

本発明は短寿命の、すなわち、有効期間が１ヶ月以内、好ましくは、１週間以内、より好ましくは１日以内、さらに好ましくは、１２時間以内、例えば、セッションごとの認証または認定のごときセキュリティー目的のため公開鍵証明書（ＰＫＣ，Ｐｕｂｌｉｃ Ｋｅｙ Ｃｅｒｔｉｆｉｃａｔｅ）を自動的に生成するシステムを提供する。

【００２８】

１つの実施例では、ユーザーが初回の認証システムを用いて認証を請求するごとに（例えば、ユーザーがログオンして、自分自身の認証を行うごとに）、新規の、しかし短寿命のＰＫＣが生成され、ユーザーに配送される。典型的には、公開鍵は比較的頻繁に（たとえば、８時間ごと、１勤務日ごと、などなど）再発行されるが、公開-秘密鍵ペアー自体には変更がなく、比較的長寿命（例えば、約１年あるいはそれ以上）である。そこで、上に述べた新規生成されたＰＫＣを、ウエブページその他のような資源へのアクセスを制御してきたシステムを含む従

来システムでＰＫＣが使われていたのと同じやり方で、使うことができる。

【００２９】

１つの実施例では、システムは短寿命ＰＫＣを配送するだけでなく、ＰＫＣの公開鍵に対応する鍵も配送する。このことはユーザーを公開鍵保管の責任から解放してくれるし、（希望とあれば、このようなハードウエア・ベースのシステムを用いてもよいが）秘密鍵をしまっておく特別のハードウエアを使用しなければならないという制約からユーザーを開放してくれる。

【００３０】

ＰＫＣは短寿命なので、ＣＲＬ処理を必要とせずに（あるいはＣＲＬ処理の必要性を減らしながら）比較的高い信頼性を達成することができる。

【００３１】

例えば、退社した従業員の場合には、システムは、そのような従業員に対してもはや（短寿命の）証明書の発行をも拒否するように構成されており、、それ以前に有効であった既発行の証明書は期限切れとなるので、ＣＲＬについてのチェックは不必要となる。

【００３２】

１つの実施例では、秘密鍵と公開鍵の両方がアクセスを要求している人のコンピューターに返され、もし希望ならばアクセスを要求している人のコンピューター内でローカルにしまわれている秘密鍵と公開鍵が物理的なスマートカードの存在をシミュレートするのに使われるという模擬スマートカードを実行することも可能である。例えばＰＫＣＳ#11（ＰＫＣＳ，Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐｔｏｇｒａｐｈｙ Ｓｔａｎｄａｒｄ＃１１）インターフェースでは、シミュレーションは、たとえばＣ－ＳＩＧＮ、Ｃ－ＶＥＲＩＦＹのようなスマートＡＰＩ（アプリケーションプログラミングインターフェース）コールを満たすような形をとることができる。

【００３３】

このようにして、本発明は、スマートカードのための比較的完成度の高いアプリケーションプログラミングインターフェース（ＡＰＩ）の利点を利用することができ、それによって、公開鍵ベースのクライアント側認証を、実際のスマート

カードというハードウエアを必要とせずに（実際のスマートカードを取得して、それを持ち歩くなどのことなく）、実行することができる。

【００３４】

１つの実施例では、例えば、カーベロスシステムに似たＴＴＰシステムが短寿命証明書生成システムとして使うように利用することができる。このようなシステムでは、パスワードベースで、（公開鍵を用いたインフラストラクチャーまたはシステムを通して防御されている資源へのアクセスを容易にするような）公開鍵システムの利点を用いて、種々のコンピューターからログオンするユーザー（「移動ユーザー」）にも対応し、一方、公開鍵に伴う秘密鍵の配布ならびに保管、ＣＲＬの維持、利用、秘密鍵の比較的低セキュリティー又は不便なやり方での保管、などの前述の困難な点を回避しつつ、カーベロス型システムのもつ幾つかの利点が組み合わされて使われている。

【００３５】

【発明の実施の形態、好適実施例の説明】

本発明の実施例の特徴を述べる前に、従来システムの特徴を最初に述べる。図１は、カーベロスシステムに用いられている認証手順を図示している。カーベロスシステムは認証にパスワードを用いているけれども、そのシステムでは、暗号化の有無にかかわらず、パスワードを決してネットワーク上に送信しないので、特別に安全なシステムである。図示の実施例では、システムは有効期間付き証明書発行サービス（下に説明する）その他の、ユーザーにが必要とする種々のサービスを含む多くのサービスを提供することができる。

【００３６】

ここに示した実施例では、特定の資源またはサービス１１２（それは、たとえば、特定のアプリケーションプログラムのようなソフトウエアサービスであることもあろうし、データであることもあろうし、特定のハードウエア資源であるかまたはそれらの組み合わさったものであるかもしれない）を使おうとする人は、そのシステムにログオンしようとして、認証を受けている人にしか知られていないパスワードを（通常は、あるプロンプトに応じて）入力する。

【００３７】

好ましくは、普通のユーザーのセッションについて、１つのセッション（通常の長さは、例えば、８－１０時間）の間にユーザーがパスワードを必要とするのはこの時だけである（もし必要であれば、例えばセキュリティーシステムについての管理タスクのような、ある特定のタスクを実行するのにパスワードの再入力を要求するようにシステムを構成することもできるが）。

【００３８】

その人は、たとえば、ローカルエリアネットワーク（ＬＡＮ）または他の通信システムを通して鍵配布センター（ＫＤＣ，Ｋｅｙ Ｄｉｓｔｒｉｂｕｔｉｏｎ Ｃｅｎｔｅｒ）１１６に接続されているクライアントコンピューター１１４を用いてログオンを試みる。それに応じて、クライアント１１４はリクエストメッセージ（ＡＳ－ＲＥＱ）１１８を鍵配布センター（ＫＤＣ）１１６に送る。

【００３９】

リクエスト１１８は、サービスをリクエストした人の名前を表しているが、パスワードを含んではいない。ＫＤＣ１１６は、暗号化された（ＴＧＴ）″Ｔｉｃｋｅｔ Ｇｒａｎｔｉｎｇ Ｔｉｃｋｅｔ″「チケット発行チケット」（ＡＳ－ＲＥＰ）（以下、有効期間付き証明書と呼ぶ）を含む１２２を返信する。

【００４０】

有効期間付き証明書は２つの主要な構成部分を含んでいる。それらはクライアントに対して証明書発行サービスに使うチケット（セッション鍵を含むその大部分はチケット発行サービスの鍵で暗号化されている）、及び、クライアント鍵で暗号化されたクライアント用ならびにチケット発行サービス用のセッション鍵である。ユーザーがある特定のサービス１１２を使うことをはじめようとすると、ＫＤＣとのいま１つの新しいトランザクションが必要となる。クライアントコンピューター１１４はチケットのリクエスト１２４（ＴＧＳ－ＲＥＱ）をＫＤＣ１１６に送信する。

【００４１】

このリクエストは、クライアントがサービスのために使うセッション鍵（そのセッション鍵はＴＧＴ内に封印されている）で暗号化された（クライアントで生成された）オーセンテイケイター、その大部分がチケット発行サービスの鍵で暗

号化されているチケット発行サービスにクライアントが使うためのチケット（これらの両方とも有効期間付き証明書１２２に含まれていた）、ならびにサービス１１２の名前、などの多くの構成要素を含んでいる。

【００４２】

これに応じて、鍵配布センター１１６はクライアントに、クライアントがサーバーを使うためのチケットを含む少なくとも部分的にはサーバーの鍵で暗号化されたチケット１２６（ＴＧＳ－ＲＥＰ）（その大部分は暗号化されている）、ならびに、クライアントとチケット発行サーバーとの間で共有されているセッション鍵で暗号化されたセッション鍵のコピー、などを送信する。

【００４３】

この点で、クライアントはサービス１１２に対するアクセスを得るのに必要となる十分な事項を持っていることになる。このことはクライアントからサービス１１２へ証明書とチケットを含むメッセージを送信することによって達成される。これに応じて、サービスは所望されたサーバーの応答をクライアントに提供する。ＫＤＣとサービス１１２だけがチケットの暗号化に使われた秘密鍵を共有していることから、サービス１１２はこのチケットを本物（オーセンティックなもの）として扱うことができる。

【００４４】

図２に示すように、公開鍵システムはまったく違った形で動作している。典型的には、ユーザーは公開-秘密鍵ペアー２０２を生成する。ユーザーは秘密鍵２０４を、たとえば、クライアントコンピューターのファイル中か、またはスマートカード上にしまうなど、多くのやり方のいずれか１つを用いて格納する。従来のシステムにおけるこのような格納は困難を引き起こすと考えられている。特定のコンピューター上のファイルへの格納は、ユーザーは秘密鍵を格納している特定のコンピューター上の秘密鍵の使用やアクセスだけが可能であるに過ぎないということから、「移動ユーザー」にとって不利になるからである。

【００４５】

すなわち、そのようなシステムは、複数の相異なるコンピューターのいずれか（例えば、ローカルエリアネットワークその他のネットワーク内の複数のノード

のいずれか）へのログオンの資格を必要とすか希望するユーザーにとっては使い勝手の悪いものであるか、または使用不可能になってしまう、がそれでもなお公開鍵システムで制御された資源の使用は可能であるということになる。さらに、コンピューター上のファイルに秘密鍵をしまうことは、たとえそれが暗号化その他の方法で保護されているとしても、そのシステムのセキュリティーの脆弱さを表すものと考えられている。

【００４６】

スマートカード上に秘密鍵をしまうことは、少なくとも理論的には移動ユーザーと両立するものであるが、多くの状況下で、スマートカードリーダーを備えたり、各種のユーザーにスマートカードの配布を行う複数の装置を備えることに伴うコストと管理上のオーバーヘッドを考えると、それは実行不可能になってしまう。

【００４７】

ユーザーは、認証機関（ＣＡ，Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）のような信頼できる存在（ｅｎｔｉｔｙ）へ、たとえばＰＫＣＳ＃１０などを通して、公開鍵を送信する。請求者の本人性（アイデンティティ）（別の通信チャンネルで（ｏｕｔ　ｏｆ　ｂａｎｄ））を証明する際に、ＣＡはＸ．５０９証明を発行してユーザーの公開鍵２１２を証明する。

【００４８】

次に、この証明はユーザーに送り返され、ここで、典型的には、当該分野技術に精通した人々によく知られているＸ．５００またはＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ　Ｄｉｒｅｃｔｏｒｙ　Ａｃｃｅｓｓ　Ｐｒｏｔｏｃｏｌ）ディレクトリのようなディレクトリに公開することによって、一般的に利用可能となる。ＣＡはまた、上に述べたように、証明書取り消しリスト（ＣＲＬ）２１４を周期的に発行する。ＣＲＬ配布のための１つの機構はＬＤＡＰを通ずるものである。

【００４９】

従来のシステムのあるものでは、資源にアクセスしようとするユーザーは秘密鍵２１８を（典型的には、自動的なやりかたで）取り出そうとする（ステップ２１８）。公開鍵システムに基づく認証についての技術において既に知られている

多くのシステムのいずれかを使って、資源制御装置が、例えば（ＣＡによって証明された）公開鍵を使って、ユーザーが適正に正しく身元確認されていることを証明する（ステップ２２２）。

【００５０】

以前のシステムでは、証明書が長寿命であるが故に、資源制御装置は証明書がすでに失効しているかどうかを判断するため、次にＣＲＬとの比較を実行する（ステップ２２４）。上に述べたように、上記比較ステップ２２４は、制御アクセスのプロセスに新たなステップの追加を必要とする。その上、特に、直近に取り消された証明書をも検出できるほど十分頻繁にＣＲＬを公表しようとすると、ＣＲＬの作成、配布、格納や、そうでなければ代わりの追跡などの管理コストが発生する。

【００５１】

従来システムにおけるこれらおよびその他の問題に対処するために、１つの実施例では、図３に示すような証明書生成システムが使われている。本件の開示説明を理解した後では、当該分野技術に精通する何人（なんぴと）にも明らかなように、多くの種々のシステムが証明書の生成に使えるが、１つの実施例では、カーベロス型システムが使われている。図３に示した実施例では、変形カーベロス型システムの１つの構成要素が鍵配布センター（ＫＤＣ）４１６である（図４）。

【００５２】

鍵配布センター４１６は図１に関連して述べられたものと同じものであってもよいが、以下に述べる手順に合わせて変形（例えば、別のソフトウエアを備える）されている。このシステムならびに図３のやり方では、最初（例えば、インストレーションのとき）、ＫＤＣ４１６は公開-秘密鍵ペアー３１２を生成する。

【００５３】

このシステムはまた証明書のテンプレート（例えば、Ｘ.５０９証明書）も生成する（ステップ３１４）。ＫＤＣ４１６は、次に、ＫＤＣ秘密鍵を使ってテンプレートに署名する。これらのステップ３１２、３１４、３１６は、従来システムのルート証明機関による手続きとほぼ同じである（しかし典型的にはネットワ

ークサーバーまたはＫＤＣによってではない）。

【００５４】

ユーザーの登録に際して、クライアント管理者はその特定のユーザーに関する長寿命の公開-秘密鍵ペアーを生成し、ユーザーの標識に関係する鍵ペアーをＫＤＣ４１６にしまう（ステップ３１８）。ユーザーが、例えば、ネットワークへのログオンによってセッションをはじめると、ユーザーはパスワードを入力し、図１に関して先に述べたように、クライアント１１４にＡＳ－ＲＥＱメッセージ１１８をＫＤＣ４１６に送信指せる（ステップ３２２）。

【００５５】

図３と図４の実施例では、ＡＳ－ＲＥＱ１１８に応じて、システムはユーザーの公開鍵を再証明する。詳しく言えば、システムはユーザー３２４に対してＸ.５０９証明書を生成し署名する。したがって、従来の公開鍵システムでは、ＣＡは、図３と図４に従って（最初の発行の際に）一度だけ証明書を生成し公開するが、一方、本システムでは、典型的には、ユーザーがシステムにログオンするごとに、ユーザーの公開鍵を含む証明書を、長い期間、何度でも、このユーザーに対して証明書のシーケンスとして生成する。

【００５６】

本発明のシステムと従来の普通の公開鍵システムとの間のいま１つの違いは、その証明書が短寿命、すなわち、従来の公開鍵システムにおける１年から２年（あるいはもっと長い）の有効期間よりかなり短く、証明書の発行後、好ましくは６ヶ月より短い有効期間、１ヶ月より短い有効期間、さらに好ましくは、１週間以下、なお、さらに好ましくは、２４時間以下、なおも、さらに好ましくは、１２時間以下、そして好ましくは発行交付から約８～１０時間の有効時間/有効日数（失効までの時間／日）を含んでいることである。

【００５７】

このような短寿命の証明書の失効日は、このようなシステムを導入している会社またはその他の事業所の必要に応じて変わるだろうし、好ましくは、証明書に対する１つかまたはそれ以上の種類の通常またはあらかじめ設定された寿命を、例えば、（適正な認証に従って）システム管理者によって設定することが可能で

ある。

【００５８】

証明書寿命の設定の方針としては、全体を通じてのセキュリティーの程度を大きく低下させず、ＣＲＬに対するチェックの頻度を下げたり、それをなくしてしまったりできるくらいの十分短い寿命で証明書の提供ができる程度になるだろうことが予想される。

【００５９】

従って、システムが、ユーザーに対して証明書（すなわち、ユーザーの公開鍵を含む証明書）を生成（または再署名）するごとに、証明書は違った有効期間を持つことになる。新しい証明書は、（同一の公開鍵のもとでは）それ以外のプロトコルを使ってもよいが、典型的には、その前の証明書が失効して、はじめて生成される。

【００６０】

その結果、本システムでは、どのあるユーザーについても、（典型的には、日ごと、あるいは、就業日ベースで）一連の証明書が発行されるが、このユーザーに対する（複数の）証明書は完全に同じものではなく、その失効の日付けや時間などの点で一つ一つ異なっている（しかし、ある一つのユーザーの公開鍵（複数）は同一であろう）。

【００６１】

このことは、一旦ある証明書が発行されると、その後、同じ公開鍵に対して証明書が異ったフォームあるいは異った情報をもって（特に、違った失効時間/日付をもって）再発行されるということが決してなかったところの以前の公開鍵システムとは対照的である。

【００６２】

１つの実施例では、あるユーザーに対する一連の短寿命証明書に他のデータが付け付け加えられたり変形されたりする。たとえば、あるユーザーがどの資源に対して使用権限が与えられているかのデータ（あるいは他の権限データ）を短寿命証明書の中に含めることができる。このような権限（オーソライゼーションインフォーメーション）の情報の１例は、ユーザーが属している１つかまたはそれ

以上のユーザーグループの情報、たとえば、そのメンバーがある資源に対して使用権限を持つかどうかを示す情報である。

【００６３】

典型的には比較的短時間の単位（たとえば、数日とか数週間）で変わるこのような権限情報は、従来の（長寿命の）証明書に含ませるには適していないと考えられているが、本発明の実施例による短寿命の証明書に含ませることは可能である。

【００６４】

証明書の生成の後、システムはクライアント１４４（ｓｉｃ正しくは１１４）に対して証明書４２２を送信または配送する（ステップ３２６）。１つの可能な実施例では、その配送は、図１に関連して述べたのと同様、（変形された）ＡＳ－ＲＥＰレスポンスの一部としてなされる。

【００６５】

ユーザーがログオンして、証明書４２２を受け取った後なら、そのユーザーが公開鍵制御資源を含んである資源に対しての認証を受けようと希望すれば、その証明書の有効期間内であるかぎり、典型的には、ユーザーは、もう１度パスワードを入れ直すことなく、何時でも証明書を使うだけで、認証を受けることができる。

【００６６】

短寿命証明書の失効の後は、そのユーザーが資源に対するさらなる認証を受けるためには、そのユーザーは、次の短寿命証明書を得るためには上述の手続き、すなわち、典型的には、パスワードの再投入の繰り返しが必要となる。

【００６７】

好ましくは、システムは証明書だけでなく、ユーザー３２８の秘密鍵も配送し、さらに好ましくは、カーベロス型システムによって生成されたセッション鍵のような共有された秘密によって保護されたユーザーの秘密鍵（すなわち、証明書が基礎としている公開鍵に対応して）も配送する。このようにして、ユーザーは図２にあるような用途に対して秘密鍵を取り出すことができる（ステップ２１８）が、しかし秘密鍵をクライアントコンピューター１１４上のファイル（そこは

、前にも注意したように比較的壊れやすい）にしまう必要はない。

【００６８】

その上、ユーザーの秘密鍵をしまうために、集中的位置選定を用意することによって、秘密鍵の集中的管理（および鍵ポリシーの実行）が可能となり、それは秘密鍵が広く配布されている形式（すなわち、個々のユーザーによって個々に保管されている）に基礎を置く従来のＰＫシステムとは対照的になっている。

【００６９】

さらに、本システムによれば、ユーザーはシステムにログオンするのに、自分自身のパスワードを使って複数台のコンピューターのいずれをも使うことができる。すなわち、このシステムは移動ユーザーも使うことができ、しかも、物理的なスマートカードを必要としない。秘密鍵と証明書の両方を持っているクライアントコンピューター１１４は公開鍵で制御された資源にアクセスすることができる４２４。

【００７０】

公開鍵-秘密鍵ペアーは多くの資源に対する認証に関連して使われる。一例として、アクセス制御の決定は、たとえば、ＰＫＣＳ＃１１アプリケーションプログラミングインターフェース５１２（図５と６）のようなスマートカードインターフェース５１８と関連してハードウエアスマートカード５１６を使うように、スマートカードの使用を含む認証プロセスにもとづいてなされる。

【００７１】

しかし、本発明はそれ以外の付加的な方法も与えることができる。図５に全体的に示した実施例によれば、ハードウエアスマートカード５１６とインターフェース５１８の代わりにか、図示してあるように、それらに加えて、模擬スマートカード･スマートカードインターフェースを使うことも可能である.。

【００７２】

アプリケーション５１４（例えば、ブラウザー５１７のような）及びＡＰＩ５１２から見れば、模擬スマートカード／スマートカードインターフェース５２２とハードウエアスマートカード･インターフェース５１６５１８との間に何の違いもないであろう。ユーザーがカード（例えば、ＰＫＣＳ＃１１ＡＰＩでＣ－Ｌ

ＯＧＩＮコールを用いて）ログインすると、ユーザーのパスワードは、ＫＤＣ４１６に対して認証し秘密鍵と新しく生成されたＸ．５０９証明書を取り出す、のに使われる（ステップ４２２）。

【００７３】

これらの証明は次にローカルに（あるいは離れて）しまわれる（ステップ５２４）。キャッシュ５２４からの証明は、スマートカードＡＰＩコール（たとえば、Ｃ－ＳＩＧＮ，Ｃ－ＶＥＲＩＦＹ）を満たすのに使うことができる。図５と６のプロセスは、比較的成熟した技術であるＡＰＩを用いながら、ハードウエアスマートカードに伴う管理上のオーバーヘッドとコストの増大をまねくことなく、ＰＫＣＳ＃１１ＡＰＩを通して、アプリケーション５１４へのトランスペアレントなアクセスを可能にしている.。

【００７４】

図７に示すように、１つの実施例では、模擬スマートカードにログインするためのプロセスは、スマートカードへのユーザーのログオンを開始すべく、クライアントアプリケーション５１４がＰＫＣＳ＃１１、ＭＳ、ＣＡＰＩ，ＣＤＳＡなどのような標準のＡＰＩを使うときに、はじめることができる。

【００７５】

本発明のプロセスは、プロセスの間に、クライアントアプリケーションによって送信され、また、受信されるメッセージ、および/または、データは、クライアントアプリケーション５１４が、図７に示されているように模擬されたスマートカードにログオンしているか、あるいは、物理的なスマートカードにログオンするかに関わらず同じである、という意味で、クライアントアプリケーション５１４に対してトランスペアレントであることが好ましい。

【００７６】

使われる特定のインターフェース５１２は、典型的には、何のクライアントアプリケーション５１４がログインを実行するか（たとえば、マイクロソフトならＭＳ－ＣＡＰＩを使おうとするだろうし、他のブラウザーあるいはアプリケーションならＰＫＣＳ＃１１または他のインターフェース７１２を使うだろう）に依存している。

【００７７】

図示の実施例では、模擬スマートカードクライアント７１４（典型的には、クライアント側コンピューターに常駐しているソフトウエアーで実行される）は、セキュリティーサーバー７１８に、典型的には、カーベロス型の認証サービスのような認証サービスを請求７１６する。

【００７８】

典型的には、模擬スマートカードクライアント７１４は、認証リクエスト７１６を形成し、送出する前にユーザーからパスワード、および/または、ログインネームを要求する。セキュリティーサーバー７１８は模擬スマートカードクライアント７１４に認証証明書を送出７２２することによって応答する。送出された認証証明書７２２は本発明の実施例、および/または、従来システムと関連して上に述べてきたものを含むことができる。

【００７９】

しかし、送出７２２された情報は模擬スマートカードクライアント７１４が模擬スマートカードサーバー７２６に対して認証するに十分なメッセージ７２４を送るべく十分なものであるのが好ましい。

【００８０】

典型的には、模擬スマートカードクライアント７１４に送られた情報７２２は、スマートカードサービス用の（先に一般的に説明したような）チケットを含んでいる。認証請求７２４の受信に応じて、模擬スマートカードサーバー７２６はスマートカードイメージ７２８を（好ましくは、暗号化して）返送する。

【００８１】

ここで使われたように、「スマートカードイメージ」は、物理的なスマートカードがシステムで、物理的なスマートカード上にしまわれたり、そこから取り出されたりする少なくとも幾つかの情報を含むものである。例としては、公開鍵、秘密鍵、対称鍵、証明書その他が含まれる。

【００８２】

１つの実施例では、スマートカードイメージは、たとえば、秘密鍵で暗号化される。次に、模擬スマートカードクライアント７１４がスマートカードクライア

ントイメージを復号化する。

【００８３】

復号化されたイメージは、例えば、公開鍵、秘密鍵、対称鍵、証明書および同様の情報を含むことができる。それらの情報のいくつかあるいは全部（秘密鍵のように特に敏感な情報含んでいることが好ましい）は、最終ユーザーだけが知っているパスワードで暗号化することができる。

【００８４】

一般的に、図７から図８において、その下にクライアントアプリケーションと書かれているブロック５１４は、クライアント側の項目、すなわち、それは、典型的には、最終ユーザーによって使われているパソコンまたはその他のコンピューター上に常駐するソフトウエアーを使っているか、または、それらから成り立っているものであり、一方、図の右側の項目はサーバー側の項目、すなわち、それは、遠隔地のネットワークネットサーバーのように遠隔地に常駐するソフトウエアーを使っているか、または、それらから成り立っているものである。

【００８５】

図７に示された実施例では、セキュリティーサーバー７１８と模擬スマートカードサーバー７２６は別々のブロックとして示されているが、１つかまたはそれ以上の別々のブロックとして示されている１つかまたはそれ以上の構成要素を、実際は、１台のサーバーコンピューター上にあるようにシステムを構成することも可能であり、例えば、セキュリティーサーバー７１８とスマートカードサーバー７２６が１台のサーバーコンピューター上にあるようにシステムを構成することも可能である。

【００８６】

このような状況であれば、ステップ２、３と４を組み合わせて、模擬スマートカードクライアント７１４が認証リクエスト７１６をセキュリティーサーバー／模擬スマートカードサーバーに送り、また、それはスマートカードイメージ７２８を（好ましくは、暗号化して）スマートカードクライアント７１４に送り返すことによって応答する、というようにすることもできる。

【００８７】

スマートカードイメージを受信すると、スマートカードクライアント７１４は、そこで、（暗号化された）スマートカードイメージ上の期限切れ公開鍵をチェックする。もし期限切れの証明書が見つかれば、模擬スマートカードクライアント７１４は、サーバー側の証明書発行期間７３４に再認証のリクエストを送る。典型的には、模擬スマートカードクライアント７１４に送り返されてくる証明は、上に述べてきたように、一般に短寿命の証明書である。

【００８８】

模擬スマートカードクライアント７１４は、そこで、スマートカードイメージ上のオブジェクトを用いて、物理的なスマートカードシステムが使われていたならば起こったであろう応答と同じやり方でクライアントアプリケーション５１４に応答し７３６、暗号化ＡＰＩ　５１２によって提供される暗号化動作を行う。

【００８９】

図７に示すように、模擬スマートカードのログインの後は、クライアントアプリケーション５１４を実行する際に、スマートカードの動作がさらに続けられる。図８Ａと図８Ｂは、このような（多くの）動作のうちの２つの有り得る例を示している。図５Ａの例では、スマートカードイメージ８１２のログインとダウンロード（一般的に図７に関連して先に述べたように行われる）に続いて、クライアントアプリケーション５１４が、例えば、公開鍵証明書８１４を生成または格納する（典型的には、標準的な暗号化ＡＰＩ　５１２を用いて）。

【００９０】

このような公開鍵証明書（クレデンシャル）は、図８Ａの実施例で、クライアントアプリケーション５１４にとってトランスペアレントなやり方で扱われる。図示の実施例では、模擬スマートカードクライアント７１４はメッセージ８１６を模擬スマートカードサーバー７２６に送り、サーバー側の模擬スマートカードイメージを更新する。これは、本発明のシステムにおける第三者の証明（クレデンシャル）を組みこむやり方、したがって、第三者認証機関（サーティフィケイションオーソリティ）について支援提供方法を説明している。

【００９１】

図８Ｂは他の１例を示している。図５Ａの実施例において、クライアントアプ

リケーション５１４は、クライアントのコンピューターにも本セキュリティーシステムのサーバー上にもない第三者認証機関８２４との通信８２２を行う。たとえば、クライアントアプリケーション５１４が証明書を得るために第三者認証機関とコンタクトすることができる。

【００９２】

しかし、このような通信８２２の後、クライアント５１４がメッセージ８１４'を格納するためにそのメッセージ送る時、本システムは、図８Ａに関連して先に述べたのと同じやり方で、模擬スマートカードサーバー７２６に格納するための情報８１６'を送ることで、模擬スマートカードの格納に備えている。

【００９３】

図９は、本発明の１つの実施例によって、模擬スマートカードシステムに新しいユーザーが登録を行うために本システムをどのように使うかを示している。図９の実施例では、管理者、たとえば、管理者サーバー９１２を用いて、証明書のテンプレート（好ましくは、このようなテンプレートを生成するためのソフトウエアーのたすけをかりて）を準備し、それを模擬スマートカードサーバー７２６（または、それに結合された格納装置９１６）上に格納すべく９１４に送出される。

【００９４】

テンプレートは少なくとも証明書の内容の一部をシステム中での用途に指定している。典型的には、テンプレートはユーザーの特徴ある名前、発行者の特徴ある名前、その他を含んでいる。

【００９５】

新しいユーザーのために最初のパスワードが生成され、好ましくは、このパスワード７２２を、ユーザーが最初のログオンを実行した後などで、そのパスワードは期限切れ状態であるものとして、そのパスワードにフラグが立てられるようにして、リセットし（したがって、、ユーザーにパスワードの変更を強制して）、セキュリティーサーバー７１８（または、それに結合された格納装置）上に格納される。

【００９６】

ユーザーに対する新しい公開-秘密鍵ペアーの生成はクライアント側コンピューターでもサーバー側（たとえば、９１２）でも実行できる。クライアント側鍵生成はサーバーコンピューターの計算負荷を軽減するのが望ましいとき使われるだろう。 しかし、特に、多くのユーザーが一時に加わった状況下では、多くの新しいユーザーを収容するようシステムを立ち上げやすくするよう、サーバー側９１２での新しいペアーを生成するのが有用であろう。上で述べたパスワードは多くのユーザーに配布される。

【００９７】

好ましくは、この配布は、アウトオブバンド（別の通信チャンネル）で（パスワードをコンピューターネットワークを通して伝送せず、各個人に会うか電話またはそれに類似の手段などで配布することで）行われるのが望ましい。それぞれの新しいユーザーが初回にシステムにログオン９２２するとき、ユーザーは、（上に述べた）彼又は彼女のパスワードの変更を要求されることが好ましい。もし鍵ペアーがそれ以前にサーバー側で生成されていなかったならば、模擬スマートカードクライアント７１４が鍵ペアーを生成する。

【００９８】

そこで、スマートカードイメージは、例えば、上に述べたのと同様な手続き８１２を用いてクライアントにダウンロードされる。次に鍵が生成され、サーバー側で、例えば図８Ａに関連して述べられたのと同様の手続き８１６でスマートカードイメージに書きもどされる。

【００９９】

以上の説明によって、本発明の多くの利点を見ることができる。本発明は公開鍵認証（オーセンティケーション）を実行可能とするターンキーソリューションを提供している。１つの実施例では、本発明は対称鍵認証を採用して、対称鍵システムによって保護することのできるアプリケーションの使用を可能にしている。本発明はクライアント側公開鍵認証の実行を秘密鍵管理と証明書取り消し問題を解決することによって実際的なものにしている。

【０１００】

本発明は、ＣＲＬを必要とせず（または、ＣＲＬの必要性を少なくして）、ま

た/あるいは、クライアント側での格納またはスマートカード秘密鍵を必要としない公開鍵認証法を提供している。本発明は、計算的にコスト高となる頻繁な新しい鍵ペアーの生成を必要とせずに、比較的頻繁な（例えば、勤務日ごとの）公開鍵証明書の発行法を提供している。

【０１０１】

本発明は、変形カーベロス、、および/あるいは、ＰＫＣＳ＃１１またはＣＤＳＡのような、ある種の以前のシステム、あるいは、以前の標準を用いて実行することができ、それによって、ある種の比較的成熟度の高い発展したシステムの利点を生かし、同時に、以前はこのようなシステムでは避けられないと考えられていた欠点を回避しながら、実行することが可能である。

【０１０２】

本発明は公開鍵システムとカーベロスシステムの両方の形のユーザーを取り扱うことができるように、それら両方の中央管理を実行する機会を提供している。本発明は、公開鍵システムの使用または実行と認証機関としての動作の両方が可能な単一のシステムを提供している。

【０１０３】

本発明の種々の変化と変形を使うことも可能である。図で示し、また、説明を加えてきた実施例は、短寿命証明書を生成し配送するのにカーベロス型システムのようなＴＴＰシステムを採用しているが、その他のシステムもまた短寿命証明書を生成し配送するのに使うことができる。

【０１０４】

違った設備が証明書を生成し配送するのに使われているごときシステムを提供することが可能である。短寿命証明書の配送が必ずしも秘密鍵またはカーベロスチケットの配送を伴うとは限らないシステムを提供することは可能である。

【０１０５】

一般に、本発明の幾つかの特徴を、その他の特徴を使うことなく、使うことは可能である。例えば、模擬スマートカードシステムを使うことなく、短寿命証明書を生成するシステムを提供すること、または、その逆のシステムを提供することが可能である。

【０１０６】

短寿命証明書は認証と関連して使われることを予想しているが、短寿命証明書を他のセキュリティー対策、権限付与、暗号化、または、たの秘匿対策およびその他と関連して使うことも可能である。短寿命証明書は主として、セッション指向なアプリケーション（インターネットサイト、ブラウザー、または公開鍵システムで管理されたサーバー）と関連して使われることを予想しているが、短寿命証明書をデータの格納とか送信（例えば、安全な電子メール）のような他の用途に関連して用いることも、少なくとも理論的には可能である。

【０１０７】

１つの例を、インターネットまたはインターネットブラウザーアクセスの用法を説明することによって示したが、スマートカードまたは模擬スマートカードはを電子メール（「eメール」）のような他の項目に関連して用いることもできる。短寿命証明書を生成するためのＫＤＣ、または他のシステムの使用が述べられたが、中程度の寿命または（標準的な）長寿命の証明書を発行するようにシステムを構成することも可能である。

【０１０８】

証明書、および／または、秘密鍵の配送がカーベロスＡＳ－ＲＥＰメッセージの１部として発生するとして述べられているが、配送をＡＳ－ＲＥＰメッセージから切り離して行うことも可能である。

【０１０９】

もし必要とあれば、秘密鍵と証明書だけをクライアントに配送するように（つまり、有効期限付き証明書、またはその他のチケットを配送せずに）システムを構成することができるし、あるいは、公開鍵の証明書とカーベロスチケットの両方の配送が必要とされ、または、要求されているのか、そうして／または、証明書と秘密鍵が必要とされ、または、要求されているのか、のいずれかをユーザーに指定させるようにシステムを構成することもできる。

【０１１０】

本発明は、好適実施例とそれらのある程度の変化と変形との形で述べられているが、その他の変化と変形もまた用いることができるものであり、以下の請求項

によって本発明は定義される。

【図面の簡単な説明】

【図１】

従来の手順に従うカーベロス型システムのブロック図

【図２】

従来のシステムによる公開鍵/スマートカード認証システムカのフローチャート

【図３】

本発明の１実施例による証明書生成とその使用を図示するフローチャート

【図４】

本図３の手順の使用を説明するシステムのある構成部分のブロック図

【図５】

本発明の１実施例による模擬スマートカードおよび/またはハードウエアスマートカードとともに用いるためのシステムのブロック図

【図６】

本発明の１実施例による模擬スマートカードおよび/またはハードウエアスマートカードとともに用いいるためのシステムのブロック図

【図７】

本発明の１実施例による模擬スマートカードにログインするためのシステムを説明するブロック図

【図８】

図８Ａ及び図８Ｂは

本発明によるシステムがどのように第三者機関公開鍵インフラストラクチャー（ＰＫＩ，Ｐｕｂｌｉｃ Ｋｅｙ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）に対する支援を提供できるかの例を説明するブロック図

【図９】

本発明の１実施例による模擬スマートカードシステムに関係するユーザー登録を説明するブロック図

【図１】

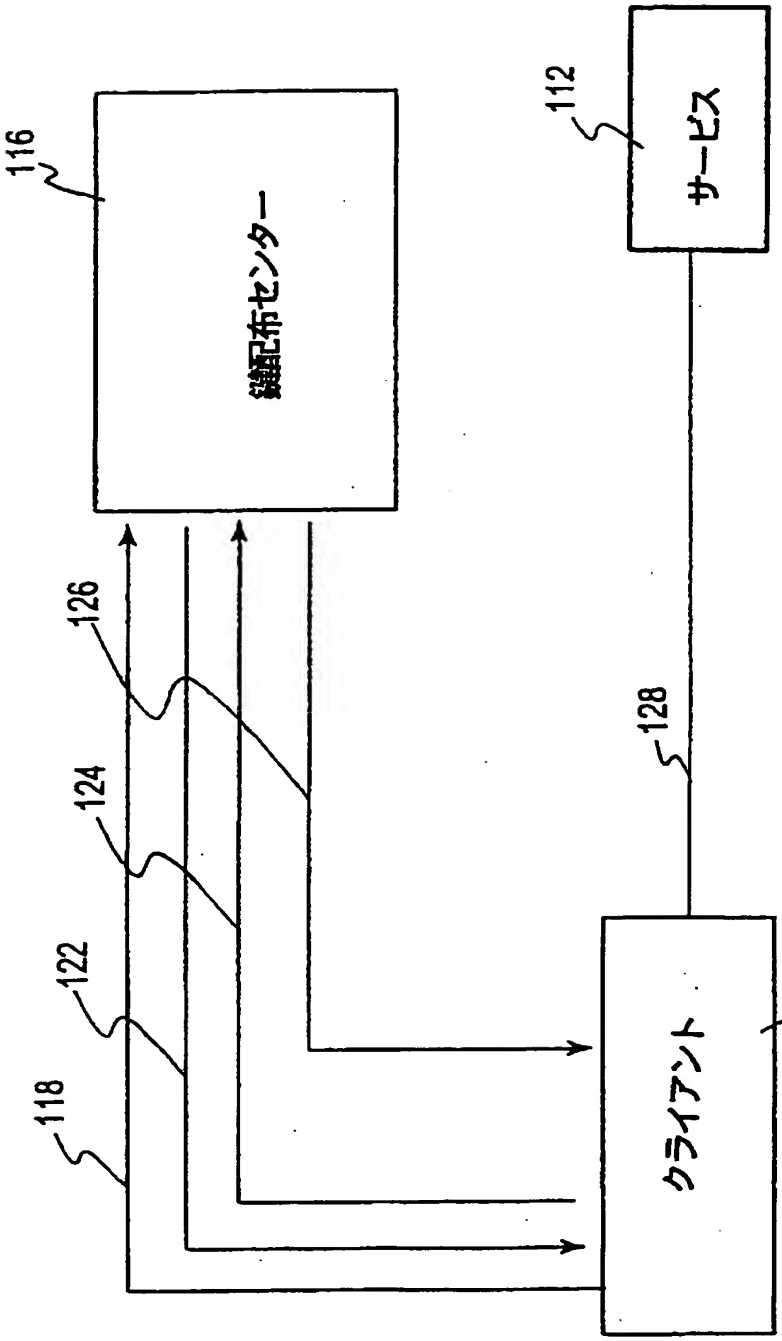
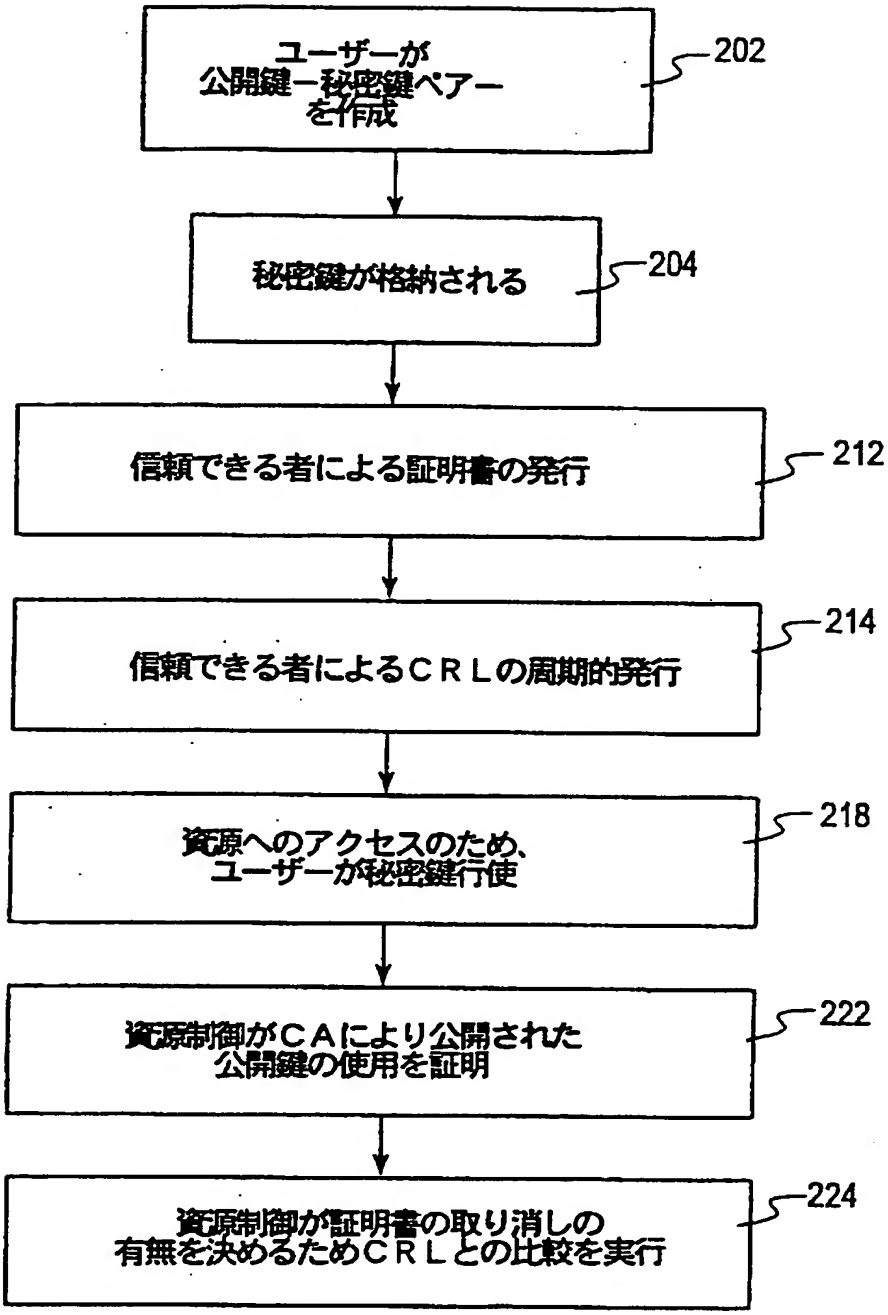


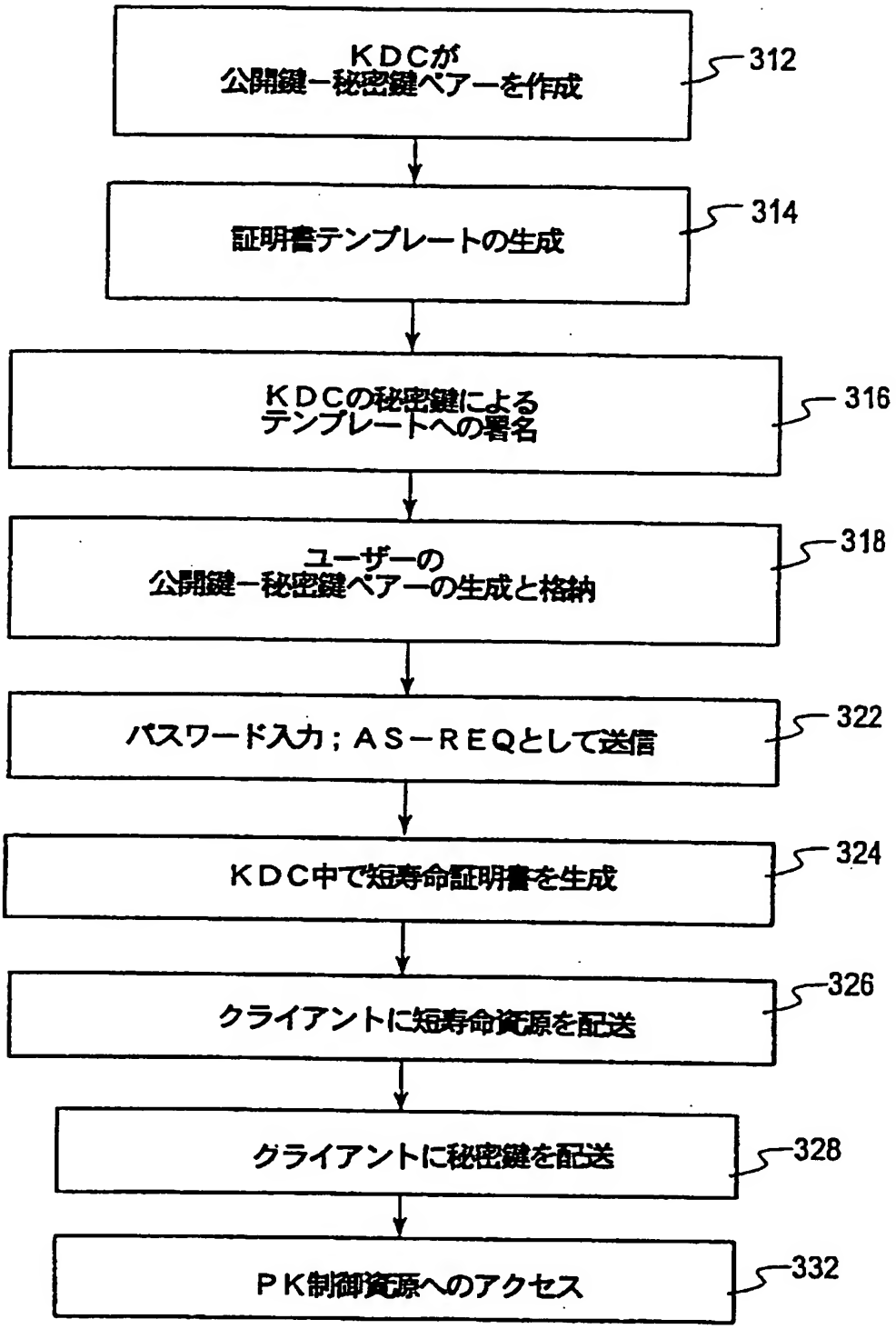
図１
先行技術

【図２】

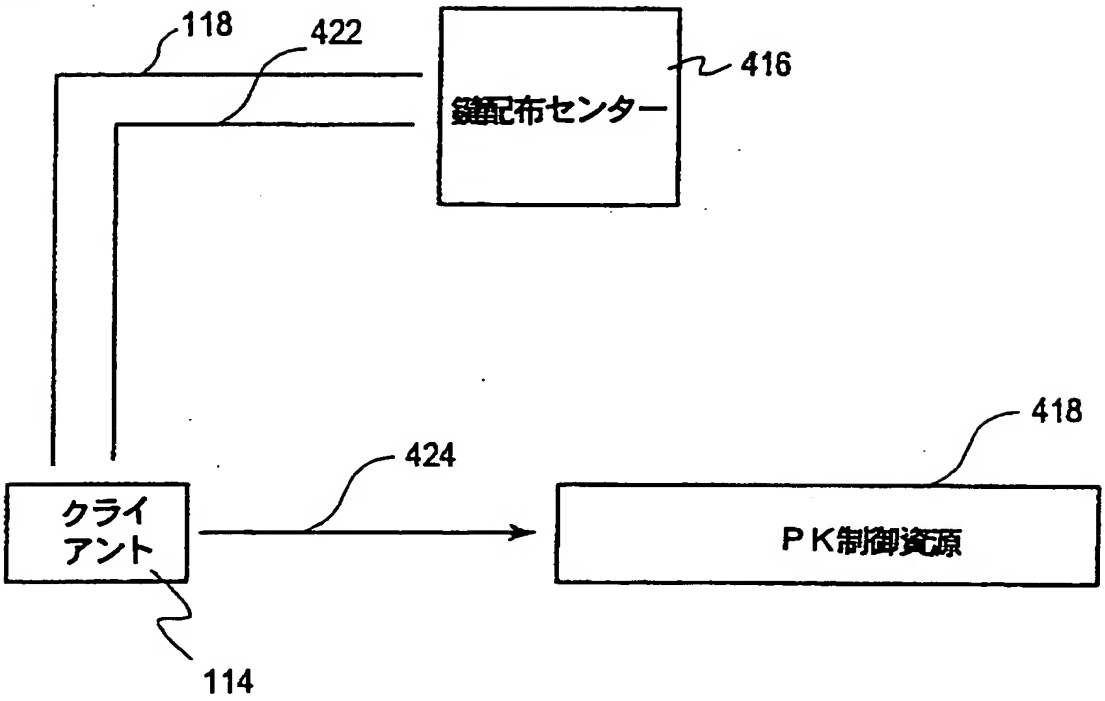

ユーザーが
公開鍵－秘密鍵ペアー
を作成
202
秘密鍵が格納される
204
信頼できる者による証明書の発行
212
信頼できる者によるＣＲＬの周期的発行
214
資源へのアクセスのため、
ユーザーが秘密鍵行使
218
資源制御がＣＡにより公開された
公開鍵の使用を証明
222
資源制御が証明書の取り消しの
有無を決めるためＣＲＬとの比較を実行
224

先行技術

【図３】


ＫＤＣが
公開鍵－秘密鍵ペアーを作成
312
証明書テンプレートの生成
314
ＫＤＣの秘密鍵による
テンプレートへの署名
316
ユーザーの
公開鍵－秘密鍵ペアーの生成と格納
318
パスワード入力；ＡＳ－ＲＥＱとして送信
322
ＫＤＣ中で短寿命証明書を生成
324
クライアントに短寿命資源を配送
326
クライアントに秘密鍵を配送
328
ＰＫ制御資源へのアクセス
332

【図４】



【図５】

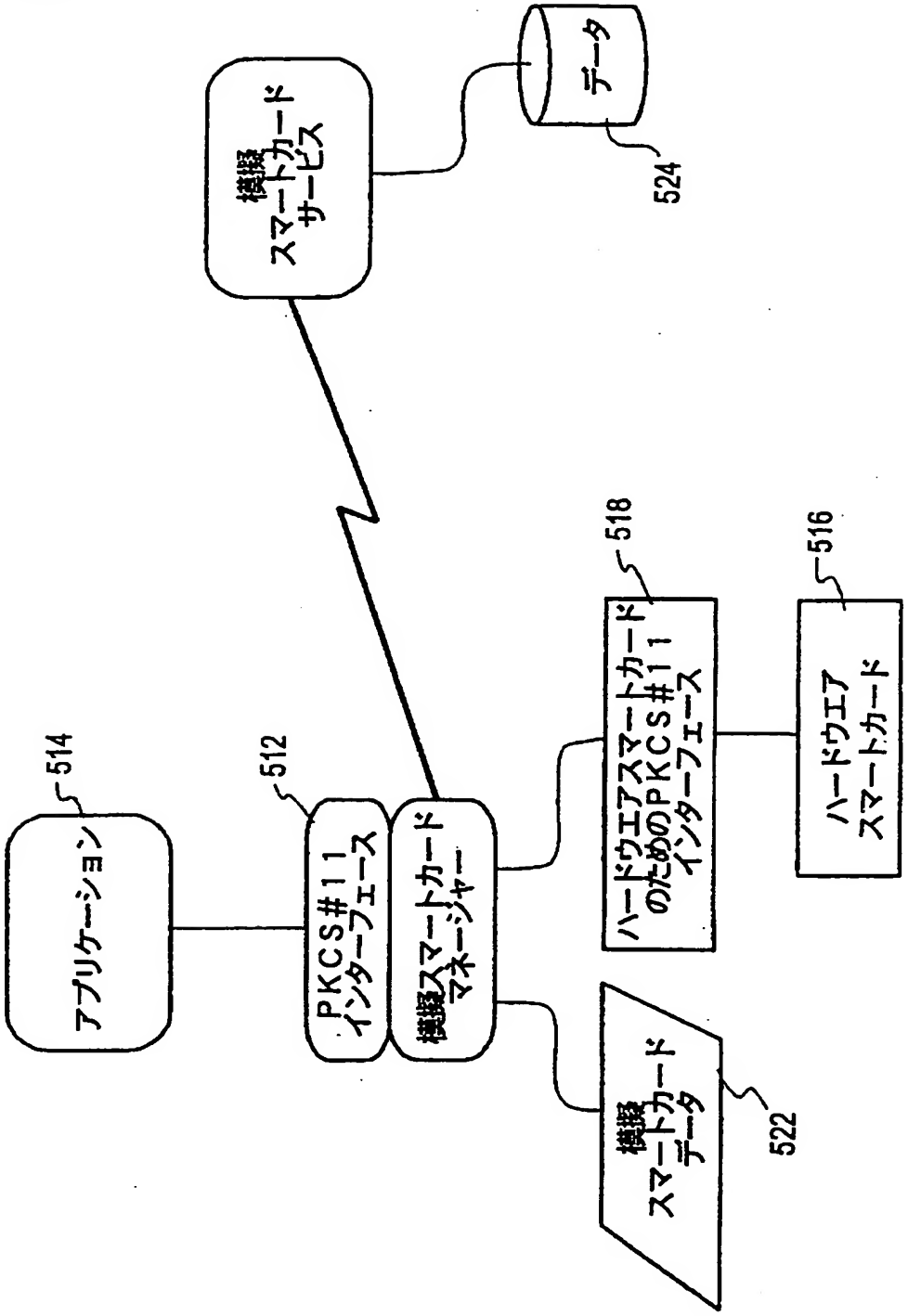

模擬
スマートカード
サービス
データ
524
アプリケーション
514
PKCS#11
インターフェース
512
模擬スマートカード
マネージャー
ハードウエアスマートカード
のためのPKCS#11
インターフェース
518
ハードウエア
スマートカード
516
模擬
スマートカード
データ
522

図５

【図６】

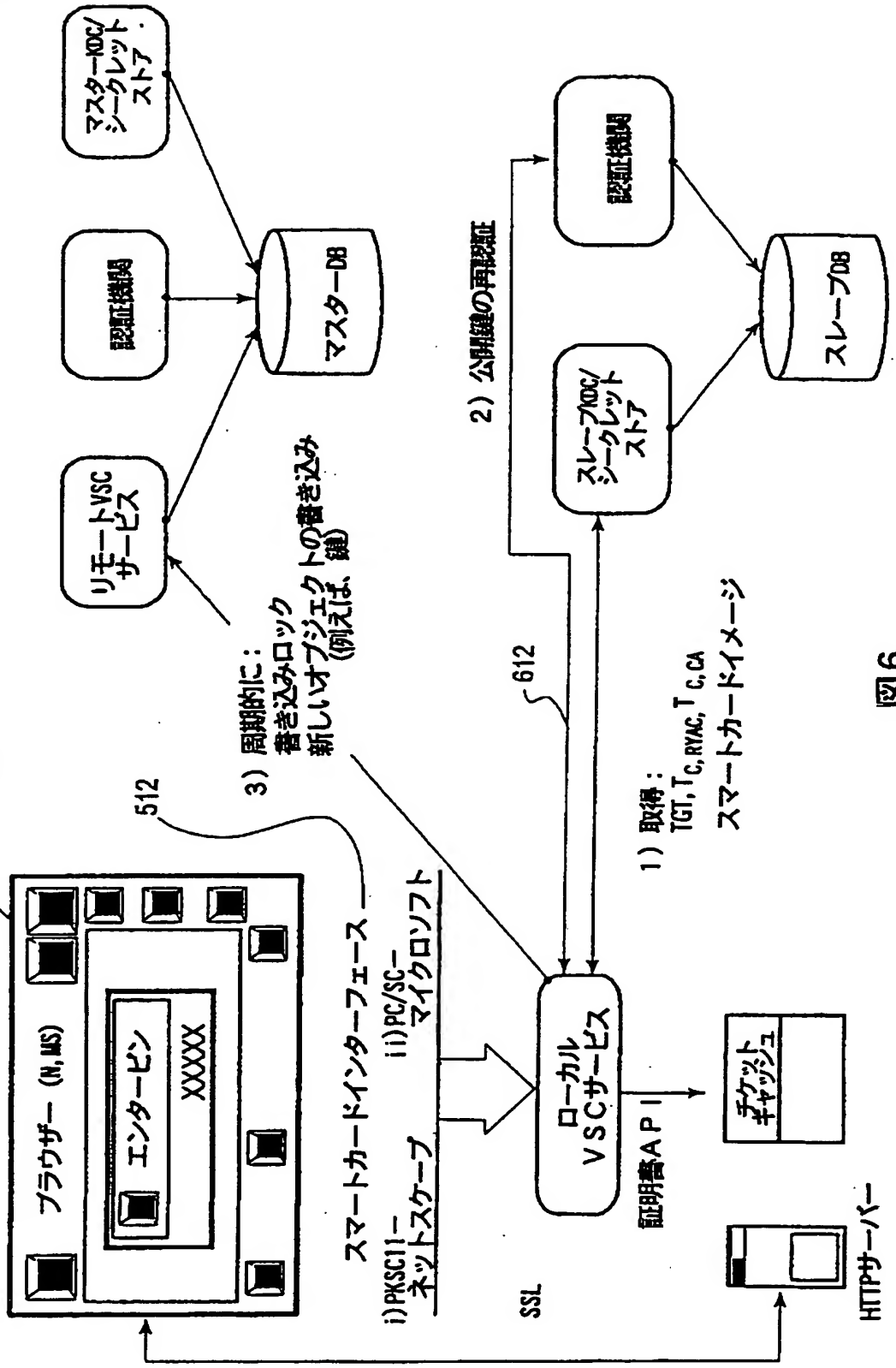

マスターKDC/シークレットストア
認証機関
マスターDB
リモートVSCサービス
3) 周期的に：
書き込みロック
新しいオブジェクトの書き込み
(例えば、鍵)
2) 公開鍵の再認証
認証機関
スレーブKDC/シークレットストア
スレーブDB
517
512
612
1) 取得：
TGT, $T_{C,RYAC}$, $T_{C,CA}$
スマートカードイメージ
ブラウザー (N, MS)
エンターピン
XXXXX
スマートカードインターフェース
i)PKSC11－ネットスケープ
ii)PC/SC－マイクロソフト
ローカルVSCサービス
証明書API
チケットキャッシュ
SSL
HTTPサーバー

図6

【図７】

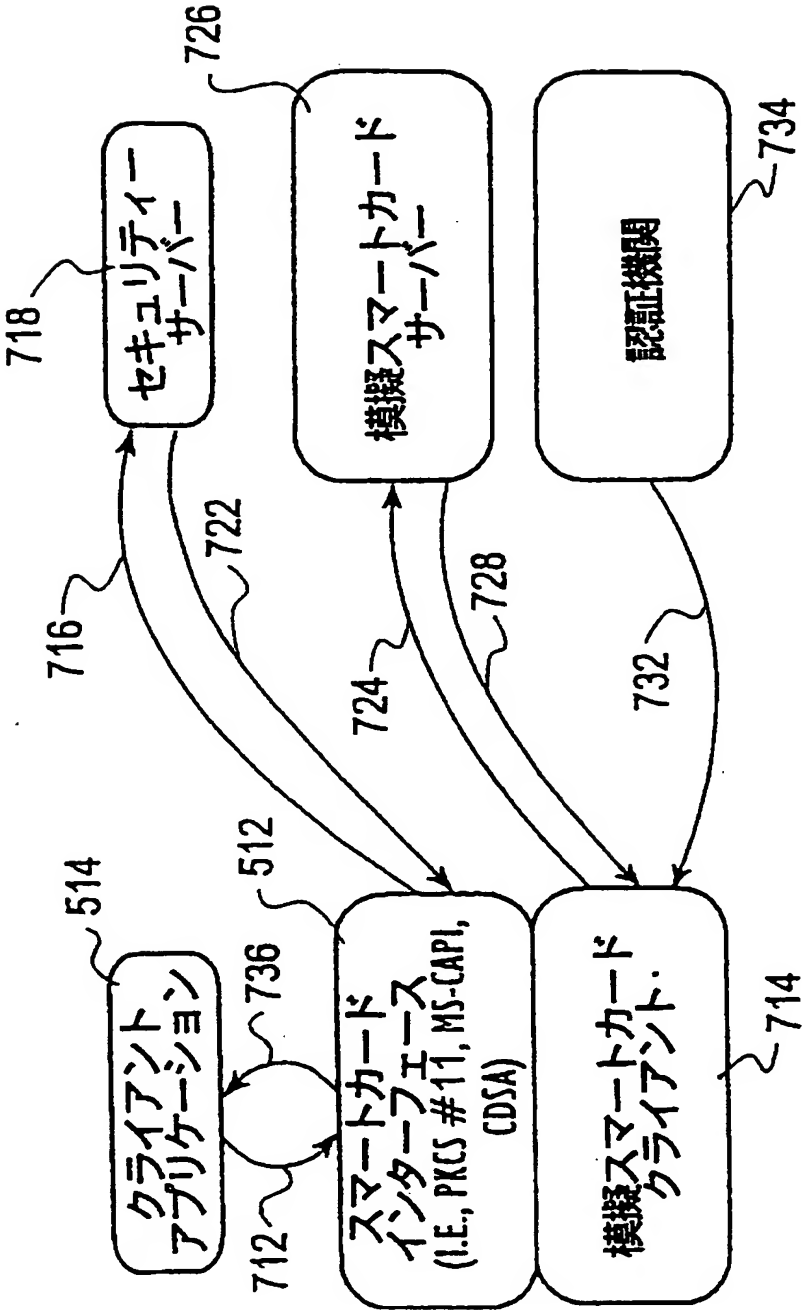

クライアント
アプリケーション
514
スマートカード
インターフェース
(I.E., PKCS #11, MS-CAPI,
CDSA)
512
模擬スマートカード
クライアント
714
セキュリティー
サーバー
718
模擬スマートカード
サーバー
726
認証機関
734
712
736
716
722
724
728
732

図７

【図８】

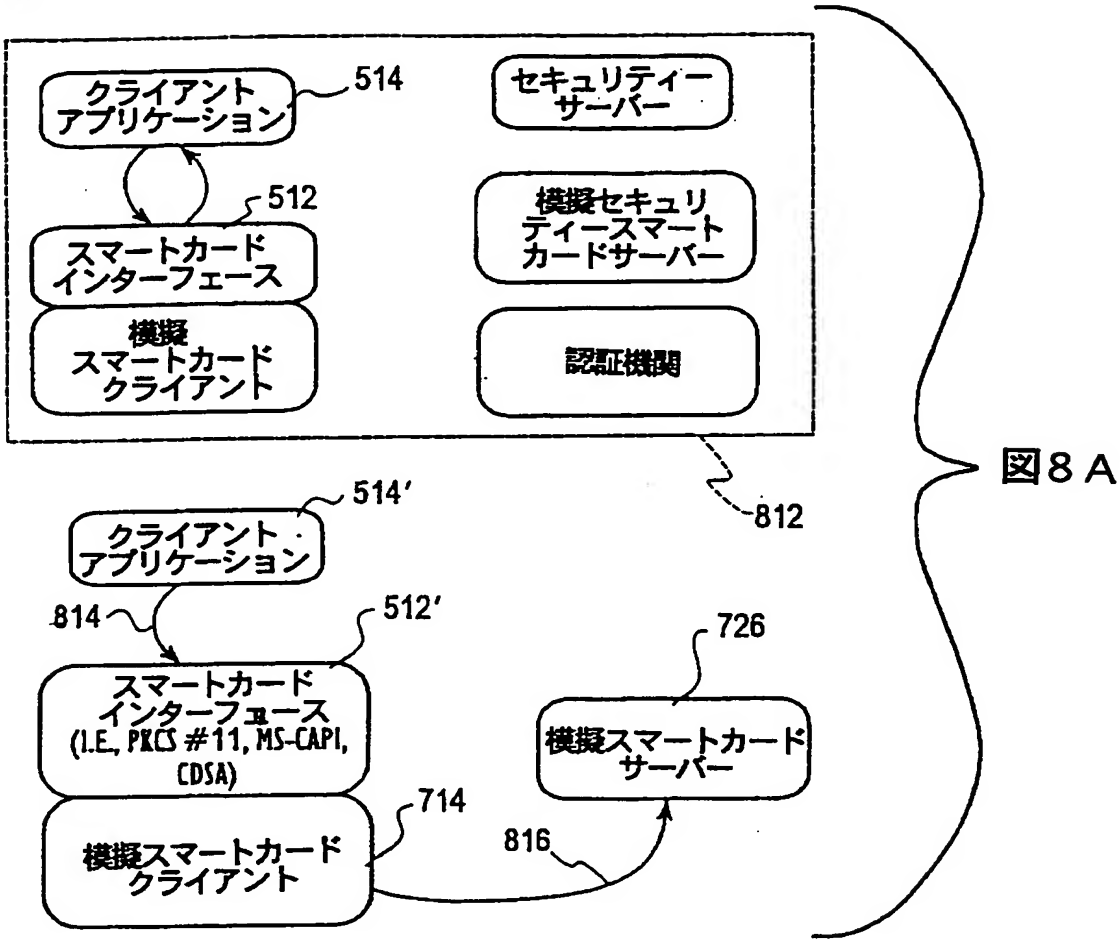

クライアント
アプリケーション
514
セキュリティー
サーバー
512
スマートカード
インターフェース
模擬セキュリ
ティースマート
カードサーバー
模擬
スマートカード
クライアント
認証機関
812
514'
クライアント
アプリケーション
814
512'
726
スマートカード
インターフェース
(I.E., PKCS #11, MS-CAPI,
CDSA)
模擬スマートカード
サーバー
714
模擬スマートカード
クライアント
816

図８Ａ

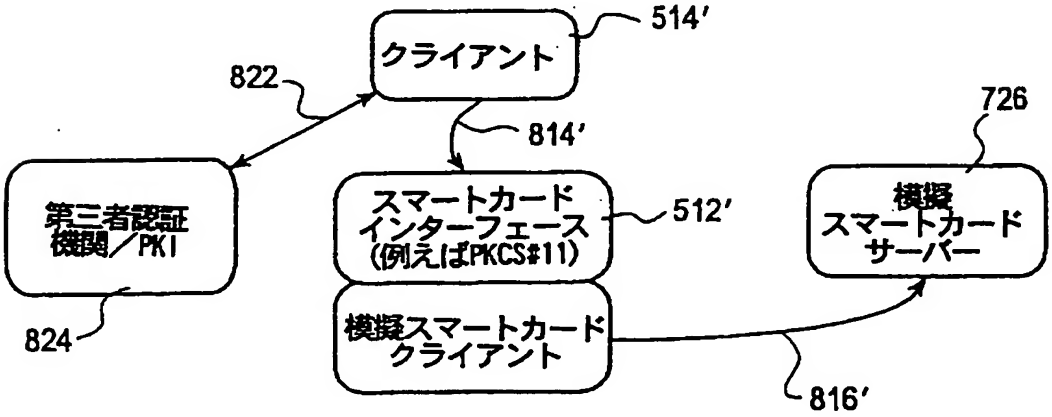

クライアント
514'
822
814'
726
第三者認証
機関／PKI
スマートカード
インターフェース
(例えばPKCS#11)
512'
模擬
スマートカード
サーバー
824
模擬スマートカード
クライアント
816'

図８Ｂ

【図９】

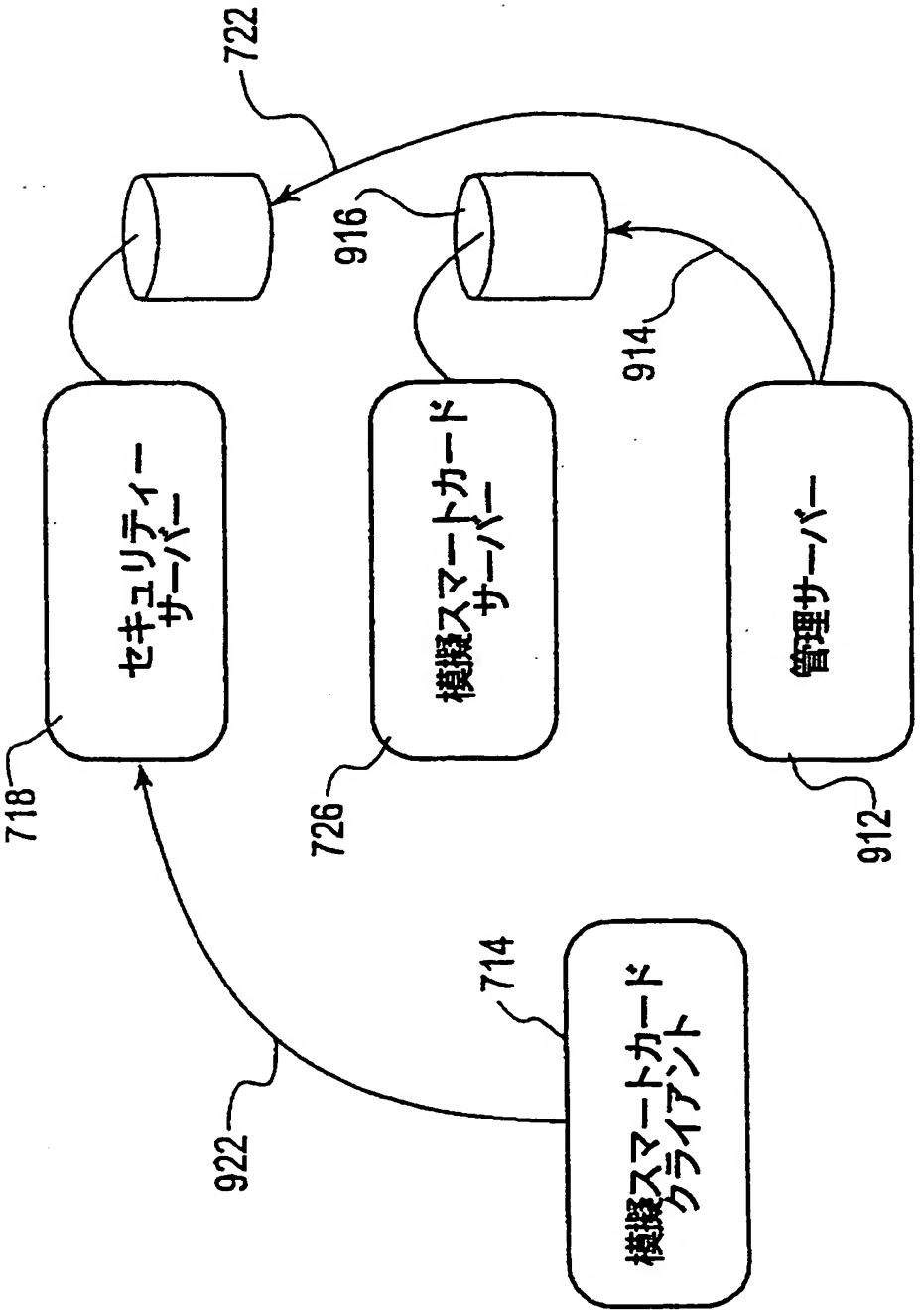

722
916
914
セキュリティー
サーバー
模擬スマートカード
サーバー
管理サーバー
718
726
912
714
模擬スマートカード
クライアント
922

図９

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/30; G06F 13/362
US CL :380/25, 30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25, 30, 21, 49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS: authenticat? and certificat?; simulat?(2w)(smart card or intelligent token)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,737,419 A (GANESAN) 07 APRIL 1998, see col. 5, lines 20-24.	1-51
A	US 5,200,999 A (MATYAS et al.) 06 APRIL 1993, see col. 90, lines 30-33.	1-51.
A	US 5,687,235 A (PERLMAN et al.) 11 NOVEMBER 1997, see col. 2, lines 24-45.	1-51
Y	US 5,347,580 A (MOLVA et al.) 13 SEPTEMBER 1994, see col. 6, lines 21-48.	52-63
Y	US 5,521,966 A (FRIEDES et al.) 28 MAY 1996, see col. 5, lines 43-55.	52-63
A	US 5,655,077 A (JONES et al.) 05 AUGUST 1997, see col. 2, lines 47-58.	52-63

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
01 APRIL 1999

Date of mailing of the international search report
20 MAY 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
GILBERTO BARRÓN JR.
Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,774,552 A (GRIMMER) 30 JUNE 1998, see col.9, lines 10-15.	1-51

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/00344

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s) 1-51, drawn to method and apparatus for issuing public key certificates.
Group II, claim(s) 52-63, drawn to method and apparatus for simulating logging in to a smartcard.
The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group I provides for the special technical feature of a short lived certificate not required in Group II. Group II provides for the special technical feature of simulating logginh in to a physical smartcard bot required in Group I.

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW

(72)発明者 コバラ，ジヨセフ，エヌ．
アメリカ合衆国，ワシントン州，イサクワ，ピー．オー．ボツクス 1027

Ｆターム(参考) 5J104 AA07 AA16 EA01 EA05 EA16
KA01 KA05 MA05 NA02 NA03
NA05 NA35 NA37 PA07